

Network Mobility and Protocol Interoperability in Ad Hoc Networks

Luiz A. DaSilva, Scott F. Midkiff, Jahng S. Park, George C. Hadjichristofi, and Nathaniel J. Davis, Virginia Polytechnic Institute and State University
 Kaustubh S. Phanse, Luleå University of Technology
 Tao Lin, McMaster University

ABSTRACT

The integration of various network-level functions, including routing, management, and security, is critical to the efficient operation of a mobile ad hoc network. In this article we focus on network mobility (rather than node mobility), implying the movement of entire subnetworks with respect to one another, while individual users initially associated with one such subnetwork may also move to other domains. One example is a battlefield network that includes ships, aircraft, and ground troops. In this “network of networks,” subnets (e.g., shipboard networks) may be interconnected via a terrestrial mobile wireless network (e.g., between moving ships). We discuss the design and implementation of a new ad hoc routing protocol, a suite of solutions for policy-based network management, and approaches for key management and deployment of IPsec in a MANET. These solutions, in turn, are integrated with real-time middleware, a secure radio link, and a topology monitoring tool. We briefly describe each component of the solution, and focus on the challenges and approaches to integrating these components into a cohesive system to support network mobility. We evaluate the effectiveness of the system through experiments conducted in a wireless ad hoc testbed.

INTRODUCTION

There has been significant research on mobile ad hoc networks (MANETs) over the past few years. Due to the complexity of the ad hoc environment, most research has focused on a single aspect of the problem, such as link establishment, medium access, routing, or mobility support. The focus of this article is on the *integration* of related functions such as network management, quality of service (QoS), routing, and security to support MANETs.

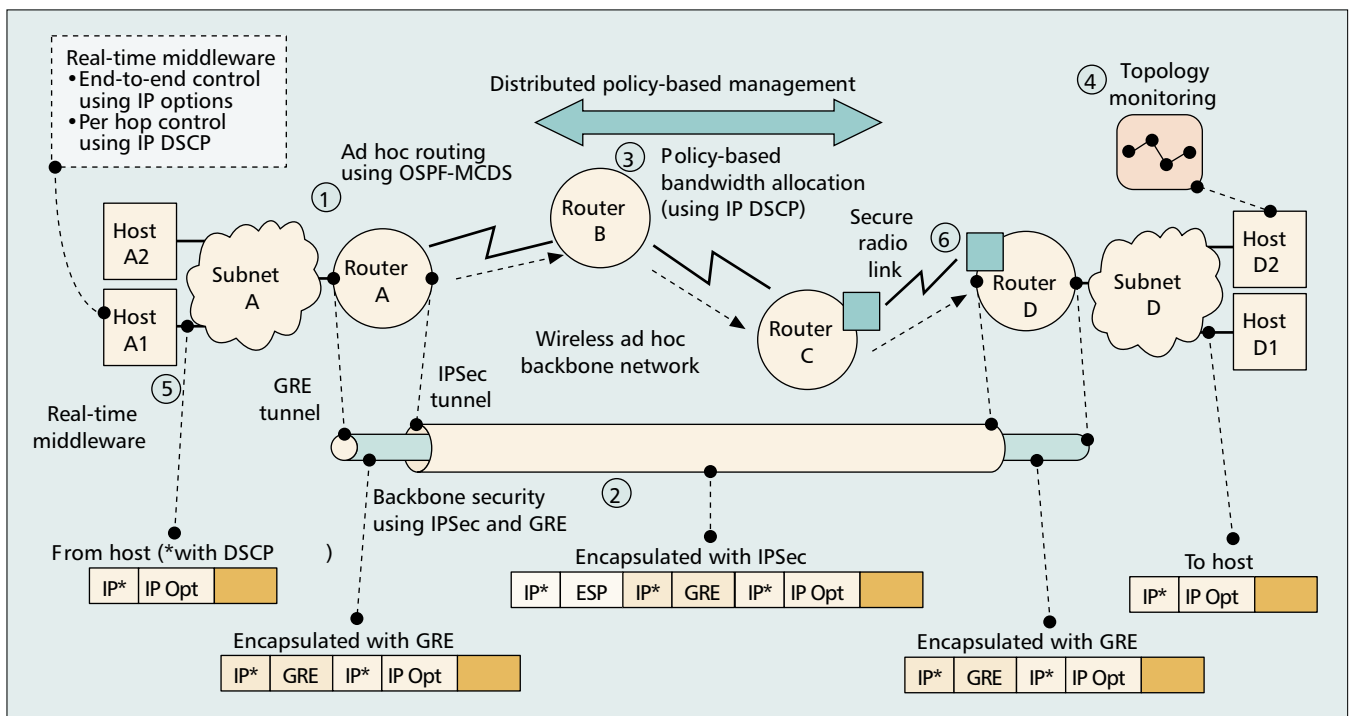
In particular, we are interested in network mobility (rather than node mobility), implying the movement of entire subnetworks with respect to one another, while individual users initially

associated with one such subnetwork may also move to other domains. One example is a battlefield network that includes ships, aircraft, and ground troops. In this “network of networks,” subnets (e.g., shipboard networks) may be interconnected via a terrestrial mobile wireless network (e.g., between moving ships). Mobile users are initially associated with their home networks but are free to move between domains. Challenges in such a scenario include interoperation among different platforms, maintenance of security associations, and distribution of policies to preserve QoS.

Figure 1 summarizes the aspects of network integration discussed in this article. We propose a modification of the Open Shortest Path First (OSPF) routing protocol:

- It uses a minimum connected dominating set (MCDS) of nodes to propagate route updates.
- Security is accomplished through the tunneling of data over the ad hoc network using Internet Protocol Security (IPsec) and Generic Routing Encapsulation (GRE). Authentication keys are dynamically distributed to network nodes using multiple key repositories.
- To achieve QoS, bandwidth is allocated according to a distributed policy-based network management mechanism.
- Some nodes in the network have the capability to perform topology monitoring through periodic exchange of Simple Network Management Protocol (SNMP) packets.
- To support real-time applications, some hosts are outfitted with middleware responsible for identifying deadline requirements of the application (associated with utility functions) and marking packets accordingly using the differentiated services (DiffServ) code point (DSCP) field of the IP header.
- Finally, a secure radio link is provided for some of the links in the network.

In this article we propose and evaluate new algorithms and protocol extensions for routing, network management, and security in MANETs. All these protocols have been prototyped and



■ **Figure 1.** Integration of network management, routing, QoS, and security in a MANET.

tested in a wireless network testbed. The evaluation was carried out through simulation as well as practical experimentation. We also describe challenges and solutions in integrating these mechanisms to form a cohesive suite of solutions in support of preserving reliability and QoS in ad hoc networks.

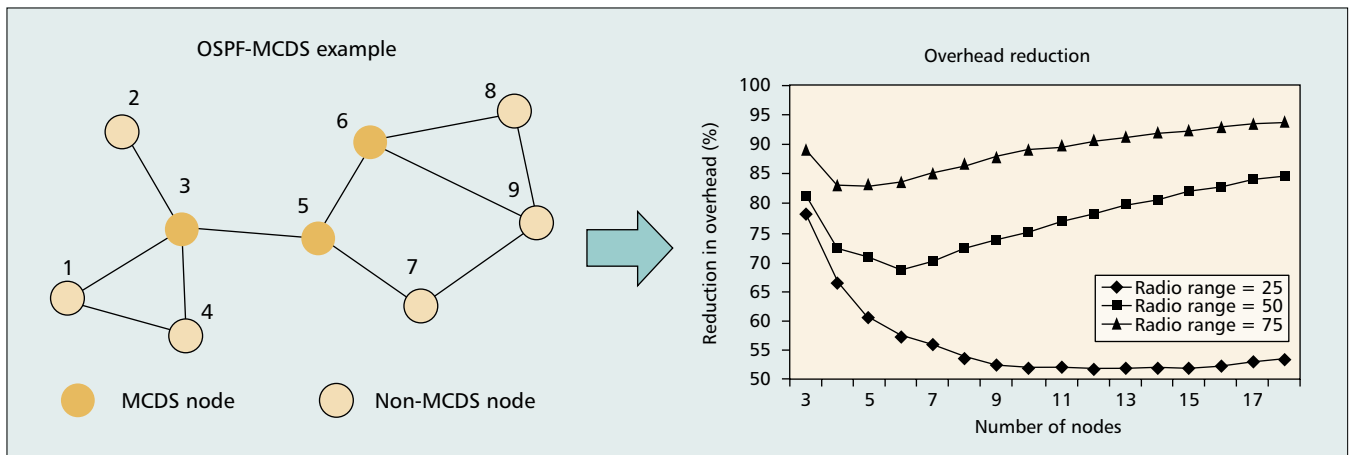
In the next three sections we summarize the main components of the solution suite: routing, policy-based network management, and security solutions. We then describe the integration of these components in a wireless testbed. We conclude by discussing major lessons learned and future directions of research.

ROUTING

A number of routing protocols have been proposed for MANETs, including Ad Hoc On-Demand Distance Vector (AODV) [1], Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) [2], and Topology Broadcast Based on Reverse Path Forwarding (TBRPF) [3]. AODV and DSR, both reactive routing protocols, cannot always provide shortest path routing since they do not update a route in use unless the route is broken due to the mobility of network components. Reactive protocols may also present high control overhead when a large number of traffic flows are present [4]. Besides these potential disadvantages, reactive protocols do not provide full topology information, which might be required by a network management application such as the policy-based management system described in the next section. Proactive routing protocols, including OLSR and TBRPF, do provide shortest path routing and more extensive topology information, at the cost of high control overhead for topology advertisements. In particular, TBRPF allows the broad-

cast of full topology information, but may produce redundant control traffic, since a node may receive the same link state information from multiple neighbors. We propose and implement a proactive protocol that locally maintains full topology information and at the same time imposes low control overhead [5].

Our proposed protocol is similar to OSPF, a widely used routing protocol designed for wired networks. We replace the concept of designated routers in OSPF by an MCDS of routers and simplify the formats of control messages [5]. We call the protocol OSPF-MCDS. A connected dominating set (CDS) is a set of routers that form a connected topology with the property that any other router not in the set has at least one neighbor in the set. Figure 2 illustrates how OSPF-MCDS works in a MANET. The set of black nodes in Fig. 2 is chosen as an MCDS. Only nodes in this set will forward any broadcast topology control messages. For example, when the link between nodes 1 and 4 becomes available, one of the end nodes, say node 1, first broadcasts the existence of this new link. The link state information is then propagated to other nodes via nodes 3, 5, and 6. By the definition of a CDS, broadcast topology control messages can reach all nodes in the network. Thus, all nodes maintain identical copies of the network topology (except for short-term inconsistencies due to delays in the propagation of control messages), and build their own shortest path trees and generate routing entries accordingly. Unlike some other protocols that use CDS nodes as default gateways for routing, such as OLSR [2], the Core Extraction Distributed Ad Hoc Routing (CEDAR) protocol [6], and the simple gateway protocol proposed by Wu and Li [7], OSPF-MCDS can generate smaller CDSs and only uses CDS nodes to broadcast topology



■ Figure 2. An example MANET running OSPF-MCDS.

information. Relay nodes in OSPF-MCDS are selected only to propagate control messages. They do not necessarily serve as gateway routers for user data packets, unlike in OLSR, where relay nodes are chosen as gateways for user data packets. When the traffic load is heavy, using CDS nodes as gateways may increase collisions between data packets and control packets, a potential problem in OLSR, CEDAR, and Wu and Li's simple gateway protocol. For a detailed explanation of the algorithm we developed to choose the MCDS, we refer the reader to [5].

Broadcast using an MCDS can reduce the number of retransmissions compared to blind broadcast (all nodes rebroadcast control messages that have not been received before) and thus achieves the goal of low control overhead. The redundant traffic eliminated by using a CDS is proportional to the number of non-CDS nodes divided by the total number of nodes in the network.

A simple simulation is presented here to illustrate the improvement [5]. In the simulation n nodes are randomly placed in a 100×100 square unit area. Radio range determines connectivity between two nodes: if radios are capable of longer transmission and reception ranges (e.g., by increasing power or antenna gain), more links are viable, resulting in a more densely connected network. Three radio ranges, 25, 50, and 75 units, are used. To find an optimum CDS for all topologies, all possible node sets are examined. The CDS with the minimum size is kept. For each set of parameters, we replicate the experiment 1000 times with different random node placements. The graph in Fig. 2 shows the percentage of overhead reduced using a CDS compared to blind broadcast. Overhead is reduced by over 50 percent for all radio ranges and values of n . Savings increase when radio range increases, implying greater benefit in dense networks. Besides the advantage of low control overhead, OSPF-MCDS also maintains shortest path routing and can provide full topology information. The link costs can optionally be defined according to traffic load or power consumption for load balancing or power efficient routing.

Using MCDS to reduce control overhead is a subject of much current research. The algorithm

we used in OSPF-MCDS exhibits better performance than other known approaches in terms of the average size of CDSs, which in turn determines the number of retransmissions of control messages, and control overhead [4, 5]. A recent simulation study reported in [4] also demonstrates that OSPF-MCDS generates low overhead compared to reactive protocols such as AODV, especially when the number of traffic flows is large.

In our integrated testbed, described later, a copy of OSPF-MCDS runs in every gateway node. It maintains a local routing table to enable subnet-to-subnet routing. Moreover, it provides hop counts between any pair of nodes to the policy-based management system discussed below.

POLICY-BASED QUALITY OF SERVICE

Unlike legacy network management, which generally involves configuring and managing each network entity individually, policy-based network management (PBNM) configures and controls the network as a whole, providing the network operator with simplified, logically centralized, and automated control over the entire network. PBNM can be used to control different networking capabilities such as QoS, network security, access control, and dynamic IP address management. A PBNM provides a viable solution for managing a mobile ad hoc internetwork: a consortium of multiple subnetworks controlled by distinct organizational policies.

We propose a solution suite [8] to apply the policy-based approach, for the first time, for managing QoS in MANETs. The four components of this suite are briefly described here.

***k*-hop cluster management:** Using clustering, we limit the number of hops between a policy server and its clients. We propose two ways to implement clustering:

- By taking advantage of the topology information gathered by the underlying proactive ad hoc routing protocol, whenever such information exists
- Through interaction between the Common Open Policy Service (COPS) protocol-based application layer and the IP layer, the idea being to control the time-to-live (TTL) field in the IP header for the COPS Keep-Alive

(KA) messages exchanged periodically by the policy server and client
Both methods enable clustering with minimal additional overhead.

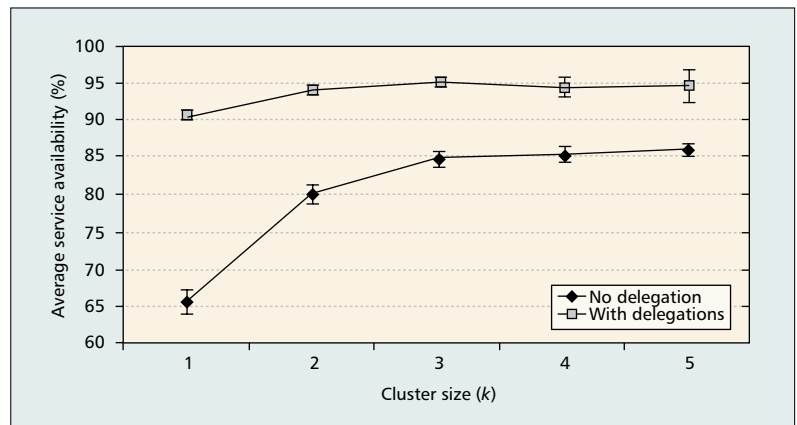
Dynamic service redundancy (DynaSeR): The DynaSeR solution implements redirection and delegation that allow the PBNM system to improve its service coverage. Redirection is a server-centric way of helping a client leaving its current cluster to discover a new server, while delegation allows dynamic invocation of policy server instances on demand to cover as many clients in the network as possible by covering those that lie outside all existing clusters. We extend the standard COPS for Provisioning (COPS-PR) protocol, adding delegation capabilities.

Service discovery: We implement a lightweight service discovery mechanism to facilitate automated discovery of policy servers in the network. Two types of messages are used: service advertisement (SA) and client service request (CSRQ). A policy server periodically advertises itself via a limited k -hop broadcast of SA messages. A client that does not receive an SA message within a certain time interval broadcasts a CSRQ message. The server, which may have moved within k hops of the client, responds with a unicast SA message. Alternatively, a client node that is currently being serviced, upon hearing a CSRQ message, may volunteer to act as a delegated server.

Interdomain policy negotiation: We extend the COPS-PR protocol to facilitate inter-policy-server communication, and to support policy negotiation between different network domains. This allows seamless QoS provisioning for nodes moving across different domains in a mobile ad hoc internetwork.

We implement our proposed schemes and protocols both as a prototype in a Linux-based ad hoc network testbed (discussed later) and as simulation models in QualNet. The PBNM system prototype is integrated with the OSPF-MCDS proactive ad hoc routing daemon to implement k -hop clustering, and its operation is demonstrated over a heterogeneous (wired and wireless) ad hoc network secured using IPsec and GRE tunneling. The effectiveness of the PBNM system in managing QoS is illustrated using soft real-time applications [9]. Almost seamless QoS is obtained for real-time applications hosted on a mobile device moving across an emulated multidomain ad hoc network. The integration between PBNM and real-time applications is further discussed in the integration section of this article.

Through simulation, we study the performance (service availability and overhead) of the PBNM system as a function of mobility, network density, and cluster size. We adopt the random waypoint mobility model to simulate node mobility. Our proposed management solution is found to scale well (up to 100 nodes were considered). The trade-off lies in increased predictability and reliability for small cluster sizes vs. improved service availability for large cluster sizes. Our proposed delegation scheme addresses this trade-off and allows the PBNM system to improve its service coverage while maintaining smaller cluster



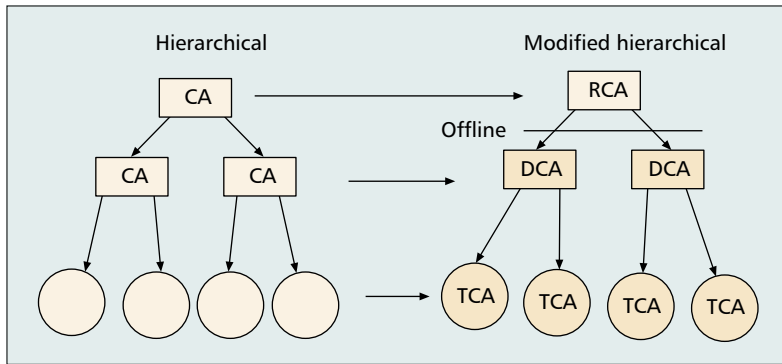
■ Figure 3. Improvement in service availability through the use of delegation.

sizes. As shown in Fig. 3, delegation improves the policy service availability by up to 25 percent. Thus, we can generally use small clusters for localized management, while catering on demand to client nodes that fall outside existing clusters. For a complete set of results, we refer the reader to [10].

SECURITY

In the security area, we focus on the interoperability of IPsec and key management over multiple platforms (Cisco, Microsoft Windows 2000, and Red Hat Linux) with different emerging technologies such as OSPF-MCDS, QoS, and real-time systems (RTS). FreeS/WAN IPsec, a freely available commercial off-the-shelf implementation of IPsec, is installed in all Linux gateways. The selection of FreeS/WAN is based on the availability of IPsec implementations for RedHat Linux and functionality. FreeS/WAN IPsec was the only version available at the time of testbed deployment. Even though there is an IPsec implementation built into the latest Red-Hat Linux kernel, that implementation lacks the functionality of opportunistic encryption that is used in our testbed. Opportunistic encryption facilitates future interoperation of FreeS/WAN IPsec with our proposed key management scheme, including the notion of trusted peers described in this section.

To deploy a security mechanism such as IPsec in a network, two peers must have a preconfigured level of trust between them. This level of trust is achieved via authentication. Using authentication, people or devices can verify each other's identity by providing proof of their identity with a preshared key or certificate. These keys or certificates can be distributed to the nodes automatically via a key management system. Key management entails the secure generation, distribution, revocation, reissuance, and storage of keys on network nodes. A MANET environment is characterized by unpredictable connectivity, node failures, and security vulnerabilities that hinder the proper operation of a key management system. In our work we address the storage and distribution aspects of key management. We also investigate ways of providing redundancy and robustness for key management to facilitate the establishment of IPsec security



■ **Figure 4.** The key management system adopts a modified PKI model.

associations in a MANET and propose a complete key management system for such an environment.

Key negotiation in our testbed is provided using automatic keying via the Internet Key Exchange (IKE) protocol [11]. Authentication is achieved using asymmetric keys, which are easier to handle than symmetric keys since ownership of public keys does not compromise security. The asymmetric keys are installed in multiple key distribution centers. A relatively new feature of IPsec implemented in FreeS/WAN IPsec known as opportunistic encryption allows this functionality, which is suited for the dynamic topology of a MANET.

Opportunistic encryption enables any two systems to authenticate each other without requiring a preshared key negotiated out of band. The public keys of nodes are stored on a Domain Name Service (DNS) server, which removes the need to set up the keys in the configuration file and decreases key management overhead. The DNS servers are set up in different subnets, so they are protected by the IPsec gateways. The DNS servers are implemented using BIND in Linux. Once communication with any peer is established, nodes can dynamically obtain each other's public key during IKE negotiation and set up security associations between them. A disadvantage of opportunistic encryption is that it is currently vulnerable to a man-in-the-middle (MITM) attack. The use of secure DNS using DNS security extensions (DNSSEC) may address this vulnerability. The interoperation of DNSSEC features with IPsec is an area of future work.

The proposed key management system also implements certificate issuance and maintenance. It differs from existing architectures because it dynamically switches from a centralized scheme of trust distribution to a more distributed scheme, which is better suited to MANETs. Authentication is achieved via asymmetric keys embedded in certification authority (CA) certificates. CA certificates offer the advantage of identifying the user as well as the IP address of a node, thus removing the need for dual authentication per host. The nodes are also assigned different levels of trust by the key management system, accounting for the fact that not all nodes in a network have the same trustworthiness.

The key management system uses a modified

hierarchical model as shown in Fig. 4. The root CA (RCA) is assumed to be offline. Any node that has an RCA certificate obtained via out-of-band methods can register into the network and act as a delegated CA (DCA). Thus, the key management system requires minimal preconfiguration of trust for the nodes. The DCAs have the responsibility of issuing, distributing, revoking, and storing certificates of nodes. Furthermore, any node in the network that is not a DCA can assume the role of a temporary CA (TCA) and sign temporary certificates for collocated nodes.

Service availability is increased in a number of ways. The system offers multiple DCAs that generate, deposit, reissue, revoke, and distribute certificates to the nodes. If all the DCAs are unavailable, a node can obtain a peer's certificate from any node that already trusts that peer. This functionality is achieved by having each node store the certificates of the nodes it trusts. Furthermore, the system decreases the frequency of certificate issuance and revocation by relaxing time constraints. Certificates are reissued whenever a node or DCA desires and are revoked whenever a node is compromised. The frequency of reissuing certificates depends on the security policy of a node or DCA. A node is motivated to reissue its certificate to reestablish its status as a trustworthy node.

This system does not necessarily require out-of-band authentication with a DCA. New nodes joining the network can simply register at a lower trust level with the DCA if they are unable to authenticate with out-of-band methods. In this way, they are motivated to register with out-of-band methods as soon as they can communicate with a DCA. In addition, the key management system is flexible enough to accommodate new nodes when the DCA is unavailable. New nodes that join the network and are preconfigured with an RCA certificate can temporarily establish trust with other nodes. If they do not possess a certificate they can obtain a temporary certificate from any of the TCAs that are physically collocated by first authenticating out of band. As a result, they can temporarily be accepted into the network until they can register at a DCA.

The key management system maintains sufficient levels of security by combining node authentication with an additional element, node behavior. A behavior-grading scheme allows each node to grade the behavior of other nodes. The key management system records and evaluates the behavior of nodes and provides credentials to negotiating peers for deciding whether they should trust each other. The behavior-grading scheme provides incentives for nodes to do what is best for them while at the same time doing what is best for the entire network. Nodes are not as dependent on strict identity verification since they have the ability to judge the trustworthiness of a peer node based on its behavior in a network. As a result, the need to renew or revoke certificates is less frequent. The effectiveness of the proposed key management in distributing trust is a subject of ongoing research.

The subnetworks in our network communicate with each other via secure tunnels. The dif-

ferent configurations that can be used to achieve this functionality are either tunnel mode IPsec or transport mode IPsec with GRE tunnels. Transport mode IPsec with GRE tunnels is not used because IPsec does not properly configure routing for the IPsec virtual interfaces when path lengths between nodes in the same subnet are greater than one. As a result, packets from one node cannot be sent to another node via peer nodes unless those two nodes are directly connected. Therefore, tunnel mode IPsec is used instead of transport mode with GRE tunnels.

Real-time systems sometimes make use of the IP options field in the IP header to encode deadline information and current latency experienced by the datagram (in our study, we supported the RTS described in [9]). However, the FreeS/WAN IPsec implementation drops packets that utilize IP options in tunnel mode, not complying with RFC 2401 [12]. To preserve the IP options field and interoperate RTS with IPsec, GRE is used in conjunction with IPsec. GRE tunnels encapsulate any network layer protocol unit, allowing its transmission over any other network layer protocol. To use GRE with IPsec, GRE tunnels are attached to the private side of the gateways so that the source and destination addresses of the packet comply with the IPsec policy (Fig. 1). Interoperability of IPsec with QoS schemes is also achieved by setting both the IPsec and GRE protocols to preserve the DSCP field in the IP header through the different levels of encapsulation. The overhead impact of GRE is an additional 24 bytes per IP packet.

Special steps must be taken to integrate MANET routing protocols with IPsec. FreeS/WAN IPsec creates a virtual interface for an IKE negotiated tunnel so that packets can be routed through that interface. One of the limitations of this implementation is that it uses routing to determine the IPsec policy to be applied to every packet. More specifically, packets destined for a particular subnet and requiring encryption have to be routed through the corresponding IPsec virtual interface for IPsec to be applied to those packets. Furthermore, MANET routing protocols modify the subnet routing entries based on dynamic topology changes. These modifications introduce interoperability issues because the IPsec virtual interface and the corresponding subnet routing entry have the same network mask. A solution to this conflict that allows IPsec to be deployed in a MANET is to assign a higher subnet mask to the IPsec interface. Thus, the subnet traffic is directed through the IPsec interface complying with the IPsec policy, and MANET routing does not interfere with the IPsec virtual interface. This method decreases the size of the subnet behind the gateway and increases the number of possible subnets. A more complete and robust solution for IPsec interoperation with MANET routing requires modifications to the IPsec implementation so that IPsec is independent of routing in the Linux kernel.

In addition to security provided by IPsec, we incorporate secure radio links developed by Virginia Tech's Configurable Computing Laboratory [13]. Secure radio links are secure configurable platforms that resist reverse engi-

neering, thus protecting both the data and the intellectual property contained in them. They provide a method for user-specific integration of secure and insecure data environments. Once the user is authenticated, the platform reconfigures itself to contain the hardware necessary to perform a user-specific function. The platforms enhance their own security by physically removing all functionality of the authenticated system when the authenticated user is absent. Authentication is achieved by integrating token-based or biometric verification into the secure platforms. This approach is currently being investigated.

INTEGRATION

In this section we describe the integration of the mechanisms described above into the wireless ad hoc network testbed illustrated in Fig. 5.

In Fig. 5 gateways G1–G7 are interconnected via a *dynamic switch*. The dynamic switch emulates a mobile wireless topology, including packet loss and constrained capacity of wireless channels [14]. It allows repeatable controlled experiments in a MANET environment with many nodes in a limited testbed area. The figure shows a particular wireless topology. By changing the switching table of the dynamic switch, gateways G1–G7 can form different topologies. The operation of the dynamic switch is transparent to each node. The nodes are stationary and connected by wires, but the protocols and applications running on the nodes behave as if they were in a MANET environment.

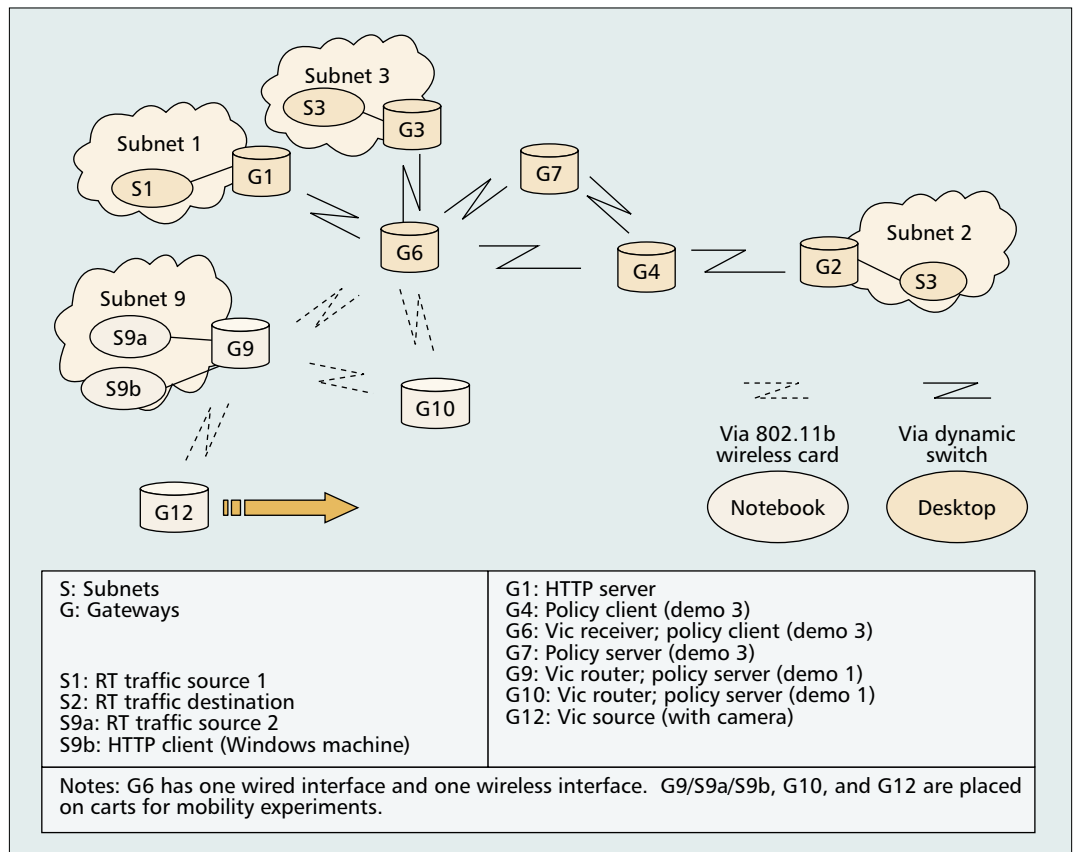
Whatever the topology may be, the connectivity of the network is maintained by the OSPF-MCDS routing protocol discussed earlier. OSPF-MCDS runs on each gateway, maintaining connectivity and ensuring the correct routing of packets with minimal overhead. A topology monitoring tool developed as part of this effort provides a real-time graphical view of the topology and the connectivity of the gateways.

A connection between any pair of gateways can be secured by using IPsec/GRE tunnels as discussed earlier. The servers and clients of the PBNM take advantage of the efficient routing protocol and secure connectivity to provide differentiated services, in terms of allocated bandwidth, to different applications. Next, we describe three test scenarios to examine the correct operation of the different protocols and the integration of these protocols.

Scenario 1 (Fig. 6) tests the performance of the OSPF-MCDS routing protocol and PBNM. It involves *true* wireless mobile nodes. Gateway 12 is initially connected to gateway 9 with bandwidth reservation that ensures a high QoS level. As gateway 12 moves toward gateway 10, OSPF-MCDS detects a new link between gateways 10 and 12, updates the topology, and maintains the connectivity. At the same time, the policy server at gateway 10 communicates with gateway 9 to provide the same level of QoS gateway 12 used to receive from gateway 9. To visualize the effects of link loss, reestablishment of the link, and QoS allocation, we transmit a video image from gateway 12 to gateway 6 via gateway 9 initially and then via gateway 10. The quality of the received video stream via gateway 10 is initially

MANET routing protocols modify the subnet routing entries based on dynamic topology changes. These modifications introduce interoperability issues because the IPsec virtual interface and the corresponding subnet routing entry have the same network mask.

As mobile ad hoc networks mature, it is necessary to integrate the various mechanisms and protocols that have been advanced into a cohesive system that supports reliable, secure communications and quality of service in this very dynamic environment.



■ Figure 5. The wireless network testbed.

poor, but as soon as the policy is negotiated, the video stream quality improves, as illustrated in Fig. 6.

Scenario 2 (Fig. 6) tests the network security capabilities of the testbed. A host connected to gateway 9 receives HTTP packets from an HTTP server in the subnet behind gateway 1. Without the IPsec tunnel between gateways 1 and 9 (via gateway 6), a hostile packet sniffer (not shown) can capture and decipher data packets over the wireless link between gateways 6 and 9. An IPsec tunnel between gateways 1 and 9 is established using IKE. During IKE negotiation the authentication keys are dynamically obtained from any of the available DNSs (S1 or S3 in Fig. 5). Once the nodes are authenticated and IPsec is deployed, the hostile packet sniffer can no longer decipher the captured packets since all packets are now encrypted.

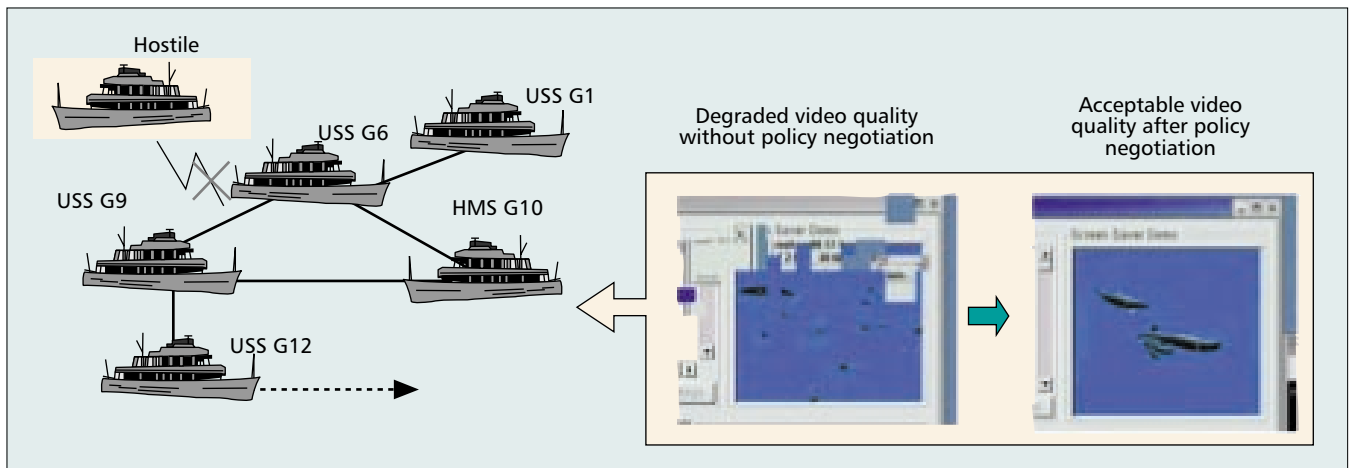
Scenario 3 tests the integration of network services and real-time middleware. Application packets are transmitted from subnet hosts of gateways 1 and 9 (S1 and S9a) to a subnet host (S2) of gateway 2. These packets are beneficial to S2 only if they arrive within the deadlines indicated by the time-utility functions marked on each packet. The policy server (at gateway 7) and clients (at gateways 4 and 6) limit the bandwidth used by background traffic and allocate sufficient bandwidth so that the application packets do not miss their deadlines. The topology and routing are provided by the OSPF-MCDS routing protocol, and the channels between gateways 1 and 2 and gateways 9 and 2 are secured by IPsec/GRE tunnels. Almost seamless QoS is

observed for real-time applications transmitted from S1 and S9a to S2.

CONCLUSIONS

As MANETs mature, it is necessary to integrate the various mechanisms and protocols that have been advanced into a cohesive system that supports reliable, secure communications and QoS in this very dynamic environment. In this article we present solutions for:

- Routing in the mobile backbone using our OSPF-MCDS protocol that is an extension of the widely used OSPF routing algorithm to support wireless interfaces and improve performance in a wireless mobile environment
 - Management of bandwidth allocation using a decentralized policy-based network management scheme
 - Secure tunnels between subnet gateways (G hosts in Fig. 5) using IPsec and GRE in a manner that is integrated with the routing and policy-based network management schemes
 - Monitoring of network topology for purposes of both testing and network management
 - Integration of PBNM with real-time middleware by using scheduling at hosts within a subnet (S hosts in Fig. 5) running the real-time middleware and supporting modified IP DiffServ in the backbone network
 - Incorporation of two secure radios to provide one link in the backbone network
- The integration of the various functions we



■ Figure 6. OSPF-MCDS, PBNM, and network security test scenarios.

describe here was not without its challenges, especially since most of the software consisted of working prototypes. Significant work went into fixing bugs as the integration proceeded. Another difficulty was the unreliable or unexpected behavior of 802.11b connections when we tested the routing protocol. The signals were sensitive to the number of people between nodes and their movement, making it difficult to obtain consistent data in different repetitions of each experiment. This experience emphasized the importance of a topology emulator like the dynamic switch described in this article for wireless testbeds. Without it, the integration would have taken much longer (and caused much more frustration).

Support for real-time applications, illustrated in Fig. 6, requires tight integration between the policy-based QoS management, security, and routing functions. For instance, the policy server's need to obtain topology information had to be considered during implementation of the OSPF-MCDS prototype. Furthermore, we use GRE tunnels to facilitate the transport of real-time traffic (whose QoS requirements are indicated using the IP options field) in IPsec tunnels. Proper configuration of the IPsec and GRE tunnels is required to ensure that the DSCP field is copied from the inner IP header to the outer IP header.

Lessons learned while investigating the security aspects in the testbed helped assess the maturity of the technology. Even though IPsec is superior for this application to other security systems such as SSL, it offered limited functionality and flexibility to systems and end users. The integration of IPsec with the various technologies required a number of adjustments to obtain the desired functionality. Some of the difficulties were due to deviation of the FreeS/WAN implementation from the IPsec architecture, as stated in RFC 2401, in conjunction with FreeS/WAN implementation limitations. Additional difficulties were due to the inability to utilize security policies and assess the state of the security associations, and the need to use dual authentication in multi-user gateways. Different mechanisms proposed in Internet drafts will likely increase the marketability of IPsec. These include an

IPsec flow monitoring management information Base (MIB), an IPsec policy information base (PIB) [15], and an IPsec information policy configuration model. However, fully functional implementations of these proposals will likely not be available in the immediate future.

Current work being undertaken as part of this project includes an experimental study of interoperation among different MANET routing protocols, an investigation of the proposed key management system with respect to both functionality and security, analytical modeling of the proposed PBNM system using stochastic Petri nets, and an extension of the management system for distributed key management.

ACKNOWLEDGMENT

This research was partially funded by the Office for Naval Research under the Navy Collaborative Integrated Information Technology Initiative (NAVCIITI).

REFERENCES

- [1] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
- [2] T. Clausen and P. Jacquet, Eds., "Optimized Link State Routing Protocol (OLSR)," IETF RFC 3626, Oct. 2003.
- [3] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," IETF RFC 3684, Feb. 2004.
- [4] T. Lin, S. F. Midkiff, and J. S. Park, "A Framework for Wireless Ad Hoc Routing Protocols," *Proc. IEEE WCNC*, vol. 2, Mar. 2003, pp. 1162–67.
- [5] T. Lin, S. F. Midkiff, and J. S. Park, "Approximation Algorithms for Minimal Connected Dominating Sets and Application for a MANET Routing Protocol," *Proc. IEEE Int'l. Perf. Comp. and Commun. Conf.*, Apr. 2003, pp. 157–64.
- [6] P. Sinha, R. Sivakumar, and V. Bharghavan, "CEDAR: Core Extraction Distributed Ad Hoc Routing," *Proc. IEEE INFOCOM*, Mar. 1999, pp. 202–09.
- [7] J. Wu and H. Li, "A Dominating-Set-Based Routing Scheme in Ad Hoc Wireless Networks," *Telecommun. Sys. J.*, vol. 18, no. 1–3, Sept.-Nov. 2001, pp. 13–36.
- [8] K. Phanse, "Policy-Based Quality of Service Management in Wireless Ad Hoc Networks," Ph.D. dissertation, Virginia Tech, Aug. 2003.
- [9] K. Channakeshava, "Utility Accrual Real-time Channel Establishment in Multihop Networks," M.S. thesis, Virginia Tech, Aug. 2003.
- [10] K. Phanse and L. A. DaSilva, "Protocol Support for Policy-Based Management of Mobile Ad Hoc Networks," *Proc. IEEE/IFIP NOMS*, Apr. 2004, pp. 3–16.
- [11] P. Hoffman, "Internet Key Exchange (IKE) Monitoring

Current work being undertaken as part of this project includes: an experimental study of inter-operation among different MANET routing protocols; an investigation of the proposed key management system with respect to both functionality and security.

MIB," IETF, draft-ietf-ipsec-ike-monitor-mib-04.txt, Apr. 2003.

- [12] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," IETF RFC 2401, Nov. 1998.
- [13] R. J. Fong, S. J. Harper, and P. M. Athanas, "A Versatile Framework for FPGA Field Updates: An Application of Partial Self-reconfiguration," *Proc. 14th IEEE Int'l. Wksp. Rapid Sys. Prototyping*, June 2003, pp. 117-23.
- [14] T. Lin, S. F. Midkiff, and J. S. Park, "A Dynamic Topology Switch for the Emulation of Wireless Mobile Ad Hoc Networks," *Proc. IEEE Conf. Local Comp. Networks (Wksp. Wireless Local Networks)*, Nov. 2002, pp. 791-98.
- [15] M. Li et al., "IPsec Policy Information Base," IETF, draft-ietf-ipsec-IPsecpib-08.txt, May 2003.

BIOGRAPHIES

LUIZ A. DASILVA [SM] (ldasilva@vt.edu) joined Virginia Polytechnic Institute and State University's (Virginia Tech's) Bradley Department of Electrical and Computer Engineering in 1998, where he is now an associate professor. He received his Ph.D. in electrical engineering at the University of Kansas and previously worked for IBM. His research interests focus on performance and resource management in wireless mobile networks and QoS issues. He is currently involved in funded research projects in the areas of QoS interoperability and policy-based network management, application of game theory to model MANETs, heterogeneous MANETs employing smart antennas, and pervasive computing, among others.

SCOTT F. MIDKIFF [SM] (midkiff@vt.edu) joined the Bradley Department of Electrical and Computer Engineering at Virginia Tech in 1986 and is now a professor. He previously worked at Bell Laboratories and held a visiting position at Carnegie Mellon University. He received his Ph.D. in electrical engineering from Duke University. His research interests include system issues in wireless and ad hoc networks, network services for pervasive computing, and performance modeling of mobile ad hoc networks.

JAHNG S. PARK [M] (jahng@vt.edu) is a research assistant professor of electrical and computer engineering at Virginia Tech. He received his Ph.D., M.S., and B.S. in electrical engineering from Virginia Tech in 2001, 1994, and 1990, respectively. He assumed his current research faculty position at Virginia Tech in 2001. His research interests are routing protocols for wireless networks, and performance evaluation of computer networks through modeling and simulations. He is a research investigator for the Navy Collaborative Integrated Information Technology Initiative (NAVCIITI) funded by the Office of Naval Research, and the Integrative Graduate Education and Research Training (IGERT) in Advanced Networking program funded by the National Science Foundation.

GEORGE C. HADJICHRISTOFI [StM] (ghadjich@vt.edu) received his M.S. degree in computer engineering at Virginia Tech in 2001 and is now working toward his Ph.D. degree. His research interests focus on network security issues, wireless networks, and mobile computing. He is currently involved in a funded research project in the areas of IPsec deployment and key management in MANETs.

NATHANIEL J. DAVIS (ndavis@vt.edu) joined the Bradley Department of Electrical and Computer Engineering at Virginia Tech in 1989 and is now a professor. He previously spent 12 years on active duty in the U.S. Army Signal Corps and was an assistant professor at the Air Force Institute of Technology. He received his Ph.D. in electrical engineering from Purdue University. His research interests include computer communication networks, computer architecture, and system performance modeling.

KAUSTUBH S. PHANSE [M] (kphanse@sm.luth.se) joined the Department of Computer Science and Electrical Engineering at Luleå University of Technology, Sweden, in January 2004 as an assistant professor. He received his M.S. and Ph.D. in electrical engineering at Virginia Tech's Bradley Department of Electrical and Computer Engineering in 2000 and 2003, respectively, and his B.E. in electronics and telecommunications from the University of Mumbai in 1998. His primary research areas of interest are wireless networks and mobile computing, QoS, policy-based network management, and delay-tolerant networks. He is a recipient of the Swedish Foundation for International Cooperation in Research and Higher Education (STINT)

scholarship for 2004.

TAO LIN [M] (taolin@ieee.org) received his Ph.D. degree in computer engineering from Virginia Tech in 2004 and is presently a post-doctoral fellow in the Electrical Engineering Department of McMaster University, Canada. He received his M.S. degree in electrical engineering from the University of Hawaii at Manoa in December 1999 and his B.S. in automation from Tsinghua University, China in August 1998. His previous research focused on the design and comparison of routing protocols for mobile ad hoc networks. His current research focuses on wireless Internet access networks and their support of real-time services for low-power mobile devices.