A Security-Aware Routing Protocol for Wireless Ad Hoc Networks

Seung Yi, Prasad Naldurg, Robin Kravets
{seungyi,naldurg,rhk}@cs.uiuc.edu
Dept. of Computer Science
University of Illinois at Urbana-Champaign
Urbana, IL 61801

Abstract— **We propose a new routing technique called Security-Aware ad hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of the routes discovered by ad hoc routing protocols. We develop a two-tier classification of routing protocol security metrics, and propose a framework to measure and enforce security attributes on ad hoc routing paths. Our framework enables applications to adapt their behavior according to the level of protection available on communicating nodes in an ad hoc network.**

I. Introduction

Wireless ad hoc networks have been proposed to support dynamic scenarios where no wired infrastructure exists. Most ad hoc routing protocols are cooperative by nature [1], and rely on implicit trust-your-neighbor relationships to route packets among participating nodes. This naïve trust model allows malicious nodes to paralyze an ad hoc network by inserting erroneous routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information [2], [3]. While these attacks are possible in fixed networks as well, the nature of the ad hoc environment magnifies their effects, and makes their detection difficult [4].

The characteristics of an ad hoc network demand new metrics for routing. Traditionally, distance (measured in hops) is used as the metric in most ad hoc route-discovery algorithms (e.g., AODV [5], DSR [6], TORA [7] etc.). The use of other metrics (e.g., geographic location [8], signal stability [9] etc.) can improve the quality and the relevance of the routes discovered for particular applications and configurations. Along these lines, we explore the use of different security attributes to improve the quality of the security of an ad-hoc route. In this paper, we present “Security-Aware ad-hoc routing (SAR)”, an approach to routing that incorporates security levels of nodes into traditional routing metrics. Our goal is to characterize and explicitly represent the trust values and trust relationships associated with ad hoc nodes and use these values to make routing decisions.

In addition to determining a secure route, the information in the routing messages must also be protected against alteration that can change routing behavior. In this paper, we analyze the security of ad hoc routing algorithms with respect to the protection associated with the transmission of routing messages. We identify the attributes of a secure route and define appropriate metrics to quantify the ”level of security” associated with protocol messages. These metrics are adapted from their equivalents in security of wired routing protocols [10], [11], [12].

In the rest of this paper, we present our motivation and the generalized SAR protocol for secure route discovery, update, and propagation. We then briefly describe our threat model, develop an attack classification, and validate our protocol against this model. Finally, we describe our experimental test bed and present our simulation results and conclusions.

II. Motivation

While the dynamics of ad hoc routing protocols have been well researched, the security issues and concerns have not been addressed in depth. In this section, we exemplify the need for security awareness in an ad hoc network at the routing level with a battlefield communication scenario.

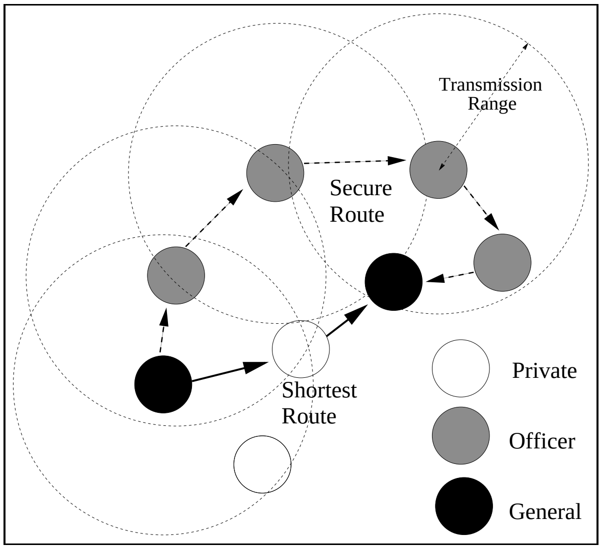

Fig. 1. Security-aware Routing - Motivation

In Fig. 1, two generals establish a route using a generic on-demand ad-hoc routing protocol. During the mission, the generals detect that some of the privates have defected. The generals decide that they can only trust nodes owned by officers to route their packets. Relaying these messages using potentially compromised nodes can leak information to untrusted entities and jeopardize the mission. Even if the generals encrypt the information flowing between them, the fact that they are communicating may disclose that a strike is imminent. Using SAR, the generals can route around the problem nodes and establish an alternate route with greater security guarantees. The sending general’s route discovery protocol embeds the rank of the node as a metric in its negotiation and tries to establish a route that avoids all privates. If the protocol can find the route, as shown in the Fig. 1, a session passing through only the officers is set up. If the protocol fails to find a route with the required security attributes or "quality of protection", it sends a notification to the sender and allows re-negotiation.

From this example, we observe that the senders or protocol initiators can make informed decisions about the "quality of protection" available to their data packets by embedding security attributes into the route discovery protocol itself. Furthermore, the quality of protection offered by the route directly affects the security of the data packets exchanged between the nodes on a particular route. Route updates and route propagation messages are also protected by this technique.

III. Security Aware Ad Hoc Routing (SAR)

We present a general description of our protocol and its behavior and enumerate the metrics we deploy to measure the quality of security of an ad hoc route discovered by our protocol. Originally, ad hoc routing protocols were based on modifications or augmentations to traditional routing protocols for wired networks [13]. These protocols send updates and react to topology changes, using monitoring and other infrastructure support to maintain routing tables. Current research focuses on pure on-demand[6], [5] routing protocols, and more recently, on augmentations that exploit additional information available on the ad-hoc nodes[8], [9], [14] to improve the quality of routes and reduce performance overheads.

Most of the protocols that have been proposed so far focus on discovering the shortest path between two nodes as fast as possible. In other words, the length of the routes is the only metric used in these protocols. Some protocols trade performance and simplified management to obtain bounded sub-optimal paths to speed up the route discovery process[15], [16]. However, the protocol metric is still the length of the routes, measured typically as hop-count. In this paper, we contend that that there are applications that require more than just the assurance that their route has the shortest length. We argue that applications must be able to specify the quality of protection or security attributes of their ad hoc route with respect to metrics that are relevant to them. Our approach shares some similarity with the policy based routing protocols for QoS[17].

A. Protocol

For simplicity, we assume that the base protocol is an on-demand protocol similar to AODV or DSR. In the original protocol, when a node wants to communicate with another node, it broadcasts a Route Request or RREQ packet to its neighbors. The RREQ is propagated to neighbors of neighbors and so on, using controlled flooding. The RREQ packets set up a reverse path to the source of the RREQ on intermediate routers that forward this packet. If any intermediate node has a path already to the RREQ destination, then this intermediate node replies with a Route Reply or RREP packet, using the reverse path to the source. Otherwise, if there exists a route (or connectivity) in the ad hoc network, the RREQ packet will eventually reach the intended destination. The destination node generates a RREP packet, and the reverse path is used to set up a route in the forward direction.

In SAR, we embed our security metric into the RREQ packet itself, and change the forwarding behavior of the protocol with respect to RREQs. Intermediate nodes receive an RREQ packet with a particular security metric or trust level. SAR ensures that this node can only process the packet or forward it if the node itself can provide the required security or has the required authorization or trust level. If the node cannot provide the required security, the RREQ is dropped. If an end-to-end path with the required security attributes can be found, a suitably modified RREP is sent from an intermediate node or the eventual destination. SAR can be implemented based on any on-demand ad-hoc routing protocol with suitable modification. In this paper, we use AODV[5] as our platform to implement SAR.

B. Behavior

Our modification to the traditional ad hoc routing protocol changes the nature of the routes discovered in an ad hoc network. The route discovered by SAR between two communicating entities may not be the shortest route in terms of hop-count. However SAR is able to find a route with a quantifiable guarantee of security. If one or more routes that satisfy the required security attributes exist, SAR will find the shortest such route. If all the nodes on the shortest path (in terms of hop count) between two nodes can satisfy the security requirements, SAR will find routes that are optimal. However, if the ad hoc network does not have a path with nodes that meet RREQ's security requirements, SAR may fail to find a route even if the network is connected.

C. Protocol Metrics

In this subsection, we enumerate different techniques to measure or specify the quality of security of a route discovered by our generalized SAR protocol. The first technique is the explicit representation of trust levels using a simple hierarchy that reflects organizational privileges. The next subsection enumerates the different techniques used to protect the integrity of routing messages in fixed-routing protocols.

C.1 Trust Hierarchy

SAR provides applications the ability to incorporate explicit trust levels into the route discovery process. Most organizations have an internal hierarchy of privileges. For example, in our battlefield scenario, the military ranks of the users of the ad hoc nodes form an explicit partial-ordering of privilege levels. A simple way of incorporating trust levels into ad hoc networks is to mirror the organizational hierarchy, and associate a number with each privilege level. These numbers represent the security/importance/capability of the mobile nodes and also of the paths. Simple comparison operators can sort these levels to reflect their position in the actual hierarchy. Another alternative is to use what we call the QoP (Quality of Protection) bit vector. For example, if mobile nodes in a network can support four different types of message protection, we can use a four bit vector to represent these message types.

However, what is more important is that this trust level or protection should be immutable. A node with a lower trust level cannot arbitrarily change its trust level, or change the trust level of the RREQ request it forwards. To provide this guarantee, many techniques can be employed. If keys can be distributed a priori, or a key agreement can be reached by some form of authentication, the simplest technique is to encrypt the portion of the RREQ and RREP headers that contain the trust level. If all the nodes in a trust level share a key, then any node that does not belong to this level cannot decrypt or process the packet, and is forced to drop it. If a node is compromised, tamper-proofing can prevent attackers from learning the values of the keys. In this paper, we leverage related research in key management for ad hoc networks and assume that some mechanism to distribute keys and share secrets is already in place.

C.2 Secure Routing Metrics

We develop our notion of the "level of protection" associated with security of information in transit in routing protocol packets. Specifically, in SAR, the aim is to protect any information or behavior that can update or cause a change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. The definition of routing protocol security used here borrows from traditional security services specifications for wired routing protocols [11]. For completeness, timeliness and ordering are added to the list of desirable security properties that can eliminate or reduce the threat of attacks against routing protocols. Techniques that can be used to guarantee these properties are also described. These are shown in Table I.

TABLE I
SECURE AD HOC ROUTING - PROPERTIES

Property	**Techniques**
Timeliness	Timestamp
Ordering	Sequence Number
Authenticity	Password, Certificate
Authorization	Credential
Integrity	Digest, Digital Signature
Confidentiality	Encryption
Non-repudiation	Chaining of Digital Signatures

The following properties can be integrated into routing protocol messages to prevent attacks that exploit the vulnerability of unprotected information in transit:

- Timeliness: Routing updates need to be delivered in a timely fashion. Update messages that arrive late may not reflect the true state of the links or routers on the network. They can cause incorrect forwarding or even propagate false information and weaken the credibility of the update information. Most ad hoc routing protocols have timestamps and timeout mechanisms to guarantee the freshness of the routes they provide.
- Ordering: Out-of-order updates can also affect the correctness of the routing protocols. These messages may not reflect the true state of the network and may propagate false information. Ad hoc routing protocols have sequence numbers that are unique within the routing domain to keep updates in order.
- Authenticity: Routing updates must originate from authenticated nodes and users. Mutual authentication is the basis of a trust relationship. Simple passwords [18] can be used for weak authentication. Each entity can append a public key certificate, attested by a trusted third party to claim its authenticity. The certifying authority can implement a password based login or a challenge-response mechanism to authenticate the identity in the first place. The receiving node can then verify this claim by examining the certificate. One of the problems in ad hoc networking is the absence of a centralized authority to issue and validate certificates of authenticity.
- Authorization: An authenticated user or node is issued an unforgeable credential by the certificate authority. These credentials specify the privileges and permissions associated by the users or the nodes. Currently, credentials are not used in routing protocol packets, and any packet can trigger update propagations and modifications to the routing table.
- Integrity: The information carried in the routing updates can cause the routing table to change and alter the flow of packets in the network. Therefore, the integrity of the content of these messages must be guaranteed. This can be accomplished by using message digests and digital signatures [10].
- Non-repudiation: Routers cannot repudiate ownership of routing protocol messages they send. A major concern with the updates is the trust model associated with the propagation of updates that originate from distant nodes. Ad-hoc nodes obtain information from their neighbors and forward it to their other neighbors. These neighbors may forward it to other neighbors and so on. In most existing protocols, nodes cannot vouch for the authenticity of updates that are not generated by their immediate neighbors. In order to preserve trust relationships, it becomes necessary to form a chain of routers (using signatures to protect integrity) and authenticate every one in turn, following the chain to the source. This is necessary because trust relationships are not transitive. Alternative solutions that avoid chaining include the path attribute mechanism developed for Secure BGP and secure distance vector routing [11], [12].
- Confidentiality: In addition to integrity, sometimes it may be necessary to prevent intermediate or non-trusted nodes from understanding the contents of packets as they are exchanged between routers. Encrypting the routing protocol packets themselves can prevent unauthorized users from reading it. Only routers that have the decryption key can decrypt these messages and participate in the routing. This is employed when a node cannot trust one or more of its immediate neighbors to route packets correctly, etc.

Each of these desirable properties has a cost and performance penalty associated with it. Some options such as enforcing access control to routing tables using credentials and providing non repudiation by chaining signatures are extremely expensive and impractical to implement and enforce in a generalized routing protocol. However, in scenarios where performance is not the driving factor, a route with quantifiable security guarantees can be more relevant than a shortest route. The purpose of this subsection was to identify the desirable properties of a secure routing protocol. SAR uses security information to dynamically influence the choice of routes installed in the routing tables. Applications can choose to implement a subset of these protection guarantees, based on a cost-benefit analysis of various techniques available to SAR in this decision making phase. In Section 5, we describe a particular implementation of SAR using AODV.

IV. Protection

We develop an attack classification and itemize the protection offered by our protocol against attacks on the trust hierarchy and the information in transit in the routing protocol messages.

A. Trust levels

Attacks on the trust hierarchy can be broadly classified as Outsider Attacks and Insider Attacks, based on the trust value associated with the *identity* or the source of the attack. SAR modifies the behavior of route discovery, tying in protocol behavior with the trust level of a user. What is also needed is a binding between the identity of the user with the associated trust level. Without this binding, any user can impersonate anybody else and obtain the privileges associated with higher trust levels. To prevent this, stronger access control mechanisms are required. In order to force the nodes and users to respect the trust hierarchy, cryptographic techniques, e.g., encryption, public key certificates, shared secrets etc., can be employed. For example, all authenticated users belonging to a trust level can share a secret key.

Traditionally strong authentication schemes are used to combat outsider attacks. The identity of a user is certified by a centralized authority, and can be verified using a simple challenge-response protocol. Various schemes including the application of threshold cryptography [2], techniques for key sharing [19], and techniques for key agreement between multiple cooperating entities in dynamic collaborative groups [20] have been proposed to tackle the lack of a centralized authority in an ad hoc network. Our open design allows us to incorporate any of these mechanisms. For example, if one key is used per level, the trust levels are immutable and the trust hierarchy can be enforced. In our implementation, for simplicity, we use a simple shared secret to generate a symmetric encryption/decryption key per trust level. Packets are encrypted using this key and nodes and users belonging to different levels cannot even read the RREQ or RREP packets. Any user or node that is an outsider cannot obtain this key.

Insider attacks are launched by compromised users within a protection domain or trust level. The users may be behaving maliciously, or their identity may be compromised (key is broken etc.). Routing protocol packets in existing ad-hoc algorithms do not carry authenticated identities or authorization credentials, and compromised nodes can potentially cause a lot of damage. Insider attacks are hard to prevent in general at the protocol level. Some techniques to prevent insider attacks include secure transient associations [21], tamper proof or tamper resistant nodes etc. For example, every time a user wants to send a RREQ, the node may require that a user re-key a password, or present her fingerprint for biometric analysis to prove her identity. If the device is lost or captured by an unauthorized user, and an attempt to send RREQs is made, this is detected by the node. The node can then destroy its keys to avoid capture (tamper proofing).

B. Information in Transit

In this subsection we examine specific threats to routing protocol *information in transit*. In addition to exploiting vulnerabilities related to the protection and enforcement of the trust levels, compromised or enemy nodes can utilize the information carried in the routing protocol packets to launch attacks. These attacks can lead to corruption of information, disclosure of sensitive information, theft of legitimate service from other protocol entities, or denial of network service to protocol entities [22]. Threats to information in transit include[23], [22], [24]:

- Interruption: The flow of routing protocol packets, especially route discovery messages and updates can be interrupted or blocked by malicious nodes. Attackers can selectively filter control messages and updates, and force the routing protocol to behave incorrectly. In SAR, a malicious node that interrupts the flow of packets belonging to a higher or lower trust level cannot cause an attack, because it is supposed to drop these packets in any case. If a node filters packets that belong to the same trust level as itself, the broadcast nature of the communication channel can help in detection of interruption attacks by other listeners within transmission range [3].
- Interception and Subversion: Routing protocol traffic and control messages, e.g., the “keep-alive” and “are-you-up?” messages can be deflected, rerouted. In SAR, the messages are protected by the key management infrastructure. In addition, the use of flooding makes these attacks superfluous.
- Modification: The integrity of the information in routing protocol packets can be compromised by modifying the packets themselves. False routes can be propagated, and legitimate nodes can be bypassed. SAR provides a suite of cryptographic techniques that can be incorporated on a need-to-use basis to prevent modification. These include digital signatures and encryption.
- Fabrication: False route and metric information can be inserted into legitimate protocol packets by malicious insider nodes. In such a situation, the sender of the RREQ may receive multiple RREPs. Currently SAR picks the first RREP that arrives at the sender. The sender can be modified to verify that the RREP has credentials that guarantee the integrity of the metrics, and repudiate the ownership of attributes by challenging the intermediate nodes. We plan to incorporate this behavior in the future.

V. Implementation

In this section, we describe an implementation of SAR, built as an augmentation to the AODV protocol in the NS-2 [25] network simulator. We retain most of AODV’s original behavior. We modify the RREQ and the RREP packet formats to carry additional security information. We call our modified AODV protocol, SAODV (Security-aware AODV).

In SAODV, RREQ packets have an additional field called RQ_SEC_REQUIREMENT that indicates the required security for the route the sender wishes to discover. This field is only set once by the sender and does not change during the route discovery phase. When an intermediate node receives a RREQ packet, the protocol first checks if the node can satisfy the security requirement indicated in the packet. If the node is secure/capable enough to participate in the routing, SAODV behaves like AODV and the RREQ packet is forwarded to its neighbors. If the intermediate node cannot satisfy the security requirement, the RREQ packet is dropped and not forwarded. When an intermediate node decides to forward the request, a new field in the RREQ packet is updated. RQ_SEC_GUARANTEE indicates the maximum level of security afforded by the paths discovered.

This approach opens the question of the effect of malicious nodes in networks. Since it is not uncommon to assume some mobile nodes will either be captured or compromised during the operation [2], SAODV must provide a way to guarantee the cooperation of nodes. This cooperation is achieved by encrypting the RREQ headers, or by adding digital signatures and distributing keys to nodes that belong to the same level in the trust hierarchy that can decrypt these headers and re-encrypt them when necessary.

The arrival of a RREQ packet at the destination indicates the presence of a path from the sender to the receiver that satisfies the security requirement specified by the sender. The destination node sends the RREP packet as in AODV, but with additional information indicating the maximum security available over the path. The value of the RQ_SEC_GUARANTEE field in the RREQ packet is copied to RP_SEC_GUARANTEE field in the RREP packet. When the RREP packet arrives at an intermediate node in the reverse path, intermediate nodes that are allowed to participate, update their routing tables as in AODV and also record the new RP_SEC_GUARANTEE value. This value indicates the maximum security available on the cached forward path. When a trusted intermediate node answers a RREQ query using cached information, this value is compared to the security requirement in the RREQ packet. Only when the forward path can guarantee enough security is the cached path information sent back in the RREP. In addition, SAODV also has support for digital signatures. If the application requested integrity support, a new field to store the computed digital signatures was added to the RREQ.

VI. Performance Evaluation

This section presents a representative sample of the simulation results collected using our SAODV implementation in NS-2 network simulator. The simulation was run for different security attributes, packet formats, traffic patterns, and trust hierarchies. Across our experiments, we observe that compared to AODV, SAODV sends fewer routing protocol control messages for the same number of flows and the same amount of application data. As a result, though the overhead per control message is higher in SAODV, the performance impact is sustainable.

A. Simulation Set-up

The results presented in this section are based on the simulation set up for 50 nodes moving around in 670m by 670m region. Nodes move according to the random way-point model described in [26]. The 50 nodes are classified into three levels (high, medium and low), each with 15, 15, and 20 nodes respectively. When a node sends out the RREQ, it uses its own security level as the security requirement for the route. In all measurements, the same amount of data (about 10000 packets) is sent, using the same number of flows (20), and sending at the same rate. The simulation is run until all flows complete sending.

Two different traffic patterns are used to drive the simulations. Traffic pattern 1 consists of 20 CBR flows. 10% of the flows are between the high level nodes, 20% between the medium and 70% between the low level nodes. Traffic pattern 2 also has 20 CBR flows, but the distribution is 33%, 33%, 34% for the high, medium, and low level nodes. The packet size is 512 bytes, and the sending rate is 4 packets/second. The maximum number of packets in each flow is 500.

B. SAODV Processing Overheads

The original AODV protocol is used as a benchmark to study the pure processing overheads of SAODV. The behavior of SAODV and AODV cannot be compared directly, since SAODV has larger RREQ and RREP packets compared to AODV and all the nodes participating in the route discovery must do additional processing. Initially, SAODV is configured to do trust enforcement processing, but not drop RREQ packets when required.

Compared to AODV, SAODV takes 1% and 3% longer to finish with traffic patterns 1 and 2. This demonstrates that the pure overhead of adding additional processing to enable security, in the absence of dropping, is not prohibitive. We use this SAODV without RREQ dropping, SAODV-D, as our baseline for rest of the performance measurements.

B.1 Path Discovery

Next, we ran SAODV-D and SAODV with explicit trust values, on the same traffic patterns to observe the difference in protocol behavior. The number of paths discovered by SAODV-D and SAODV, and the number of paths that violate the security requirement in SAODV-D were recorded. Since SAODV-D behaves like original AODV, some of the paths found violated the security requirement. This is summarized in Table II. Though SAODV-D found more paths when the trust levels were enforced, 14 and 19 of these paths respectively were unusable. SAODV discovered fewer paths, but these paths are guaranteed to obey the trust requirements of their senders.

TABLE II
Number of Paths and Security Violations

Traffic	1	2
Paths by SAODV-D	93	95
Security violation by SAODV-D	14	19
Paths by SAODV	80	73

B.2 Routing Message Overheads

Table III shows the numbers of routing protocol messages in SAODV-D and SAODV. We observe that there is a drop in the number of RREQ messages sent in SAODV. This is because the RREQ is dropped and not forwarded when the intermediate nodes cannot handle the security requirement of the RREQ packets. These results imply that SAODV generates fewer routing messages, while enabling applications to find more relevant routes. In the case of Pattern 1, there was a decrease of 2% in RREQ messages and 25% in RREP messages. For Pattern 2, the results were more accentuated (41% in RREQs, and 27% in RREPs). This is due to the fact that the trust hierarchy is more equitably distributed in Pattern 2 and paths tend to be smaller.

TABLE III
ROUTING MESSAGE OVERHEAD

	RREQ		RREP		Total	
Traffic	1	2	1	2	1	2
SAODV-D	2333	2566	107	102	2410	2668
SAODV	2285	1504	80	73	2365	1577

B.3 Overall Simulation Time and Transmitted Data

SAODV security restrictions may force packets to follow longer, but more secure paths and result in taking more time to finish communication. The overhead of the protocol is illustrated in Table IV, which shows the overall time to complete transmission of all the traffic flows in both SAODV with RREQ dropping and SAODV-D, and the total amount of data transmitted. With RREQ dropping, SAODV takes 2.3% and 0.2% more time to finish in traffic patterns 1 and 2 compared to SAODV-D. Although SAODV takes marginally more time to finish communication, it still finds paths in most cases and delivers almost the same amount of data from senders to the receivers.

TABLE IV
OVERALL SIMULATION TIME AND TRANSMITTED DATA

	Simulation Time		Transmitted Data	
Traffic	1	2	1	2
SAODV-D	2844	2918	10023	10022
SAODV	2911	2925	10028	10017

C. *Secure Routing Measurements*

The SAODV protocol is augmented with hash digests and symmetric encryption mechanisms. The signed hash digests provide message integrity, whereas encrypting packets guarantees their confidentiality. Nodes that have the same trust level share the same encryption and decryption keys. The MD5 Hash algorithm and the Blowfish block cipher were used for these measurements. We present the measurements for Traffic Pattern 1 only, due to space constraints. The results for Pattern 2 show a similar trend. The entire RREQ packet was encrypted, with the exception of the packet-type field. The SAODV-D protocol reflects the overhead of adding the extra field in the header. In Table V, we observe that SAODV-E (SAODV with Encryption) and SAODV-S (SAODV with Signed Hash) sent fewer RREQs and RREPs than SAODV-D. This is because nodes that were not capable of decrypting the encrypted RREQ packets, or could not verify the signatures, dropped these packets without forwarding. SAODV-E showed a 9.1% decrease and SAODV-S showed a 17% decrease. This reinforces our claim that SAODV sends fewer control messages (RREQs and RREPs) than SAODV-D, though each packet needs more processing.

VII. CONCLUSION

SAR enables the discovery of secure routes in a mobile ad hoc environment. Its integrated security metrics allow applications to explicitly capture and enforce explicit cooperative trust relationships. In addition, SAR also provides customizable security to the flow of routing protocol messages themselves. Routes discovered by SAR come with "quality of protection" guarantees. The techniques enabled by SAR can be easily incorporated into generic ad hoc routing protocols as illustrated by our implementation example - SAODV. The processing overheads in SAR are offset by restricting the scope of the flooding for more relevant routes, providing comparable price/performance benefits.

REFERENCES

[1] E. M. Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," *IEEE Personal Communications*, Apr. 1999.

[2] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network Magazine*, Nov. 1999.

[3] S. Marti and T. Giuli and K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile ad hoc networks," in *The Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Boston, MA, USA, Aug. 2000.

[4] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," in *The Sixth Annual ACM/IEEE Conference on Mobile Computing and Networking*, Boston, MA, USA, Aug. 2000.

[5] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," in *The Second IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, USA, Feb. 1999.

[6] J. Broch and D. B. Johnson, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," IETF Internet Draft, October 1999.

[7] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," in *The 16th Annual Joint Conference of the IEEE Computer and Communications Societies*, Kobe, Japan, Apr. 1997.

[8] Y. Ko and N. H. Vaidya, "Location-Aided Routing(LAR) in Mobile Ad Hoc Networks," in *The Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, TX, USA, Oct. 1998.

[9] R. Dube and C. D. Rais and Kuang-Yeh Wang and S. K. Tripathi, "Signal stability-based adaptive routing (SSA) for ad hoc mobile networks," *IEEE Personal Communications*, Feb. 1997.

[10] S. Murphy and M. Badger and B. Wellington, "OSPF with Digital Signatures," RFC 2154.

[11] B. Smith, S. Murthy, and J.J. Garcia-Luna-Aceves, "Securing the Border Gateway Routing Protocols," in *Global Internet '96*, London, UK, Nov. 1996.

[12] B. Smith and S. Murthy and J.J. Garcia-Luna-Aceves, "Securing Distance Vector Routing Protocols," in *Internet Society Symposium on Network and Distributed System Security, the 7th International Workshop on Security Protocols*, San Diego, CA, USA, Feb. 1997.

[13] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, 1994, pp. 234–244.

[14] S. Singh and M. Woo and C. S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," in *The Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, TX, USA, Oct. 1998.

[15] Z. Haas and M. Pearlman, "The zone routing protocol (ZRP) for ad hoc networks," Internet draft, draft-zone-routing-protocol-00.txt, 1997.

[16] P. Sinha and R. Sivakumar and V. Bharghavan, "CEDAR: a Core-Extraction Distributed Ad Hoc Routing algorithm," in *The 18th Annual Joint Conference of the IEEE Computer and Communication Societies*, New York, NY, USA, Mar. 1999.

[17] E. Crawley and R. Nair and B. Rajagopalanand and H. Sandick, "A Framework for QoS-based Routing in the Internet," RFC 2386, August 1998.

[18] J. Moy, "OSPF Version 2," RFC 2326, April 1998.

[19] N. Asokan and P. Ginzboorg, "Key-Agreement in Ad-hoc Networks," in *The Fourth Nordic Workshop on Secure Computer Systems*, 1999.

[20] Y. Kim and A. Perrig and G. Tsudik, "Simple and fault-tolerant key agreement for dynamic collaborative groups," in *ACM Conference on Computer and Communications Security*, 2000, pp. 235–244.

[21] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," in *The 7th International Workshop on Security Protocols*, Cambridge, UK, Apr. 1999.

[22] J. Howard, *An Analysis Of Security Incidents On The Internet 1989 - 1995*, Ph.D. thesis, Doctor of Philosophy in Engineering and Public Policy, Carnegie Mellon University, Apr. 1997.

[23] F. Wang, Brian Vetter, and Shyhtsun Felix Wu, "Secure routing protocols: Theory and practice," Technical Report, North Carolina State University.

TABLE V

ROUTING MESSAGE OVERHEADS FOR SECURE ROUTING

	RREQ		RREP		Routing Msgs	
	Encryption	Signed Hash	Encryption	Signed Hash	Encryption	Signed Hash
SAODV-D	2225	2219	77	85	2378	2381
SAODV	2175	2148	74	80	2341	2311

[24] W. Stallings, *Network and Internetwork Security Principles and Practice*, Prentice Hall, Englewood Cliffs, NJ, 1995.

[25] "The Network Simulator - NS-2," http://www.isi.edu/nsnam/ns/.

[26] J. Broch, D. A. Maltz, D. B. Johnson, Yih-Chun Hu, and J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," in *The Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, TX, USA, Oct. 1998.