

Security-Aware Ad hoc Routing for Wireless Networks

Seung Yi
Dept. of Computer Science
University of Illinois at
Urbana-Champaign
seungyi@cs.uiuc.edu

Prasad Naldurg
Dept. of Computer Science
University of Illinois at
Urbana-Champaign
naldurg@cs.uiuc.edu

Robin Kravets
Dept. of Computer Science
University of Illinois at
Urbana-Champaign
rhk@cs.uiuc.edu

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.

Keywords

MANET, Ad-hoc routing protocol, Security

1. 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 [2], 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 [8]. 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 [14].

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 [6], DSR [4], TORA [11] etc.). The use of other metrics (e.g., geographic location [13], signal stability [7] 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 [9, 10].

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 preliminary results and conclusions.

2. MOTIVATION

Communication among nodes in an ad hoc network is accomplished with support from the routing protocol. While the dynamics of these 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.

In Figure 1, two generals establish a route to communicate among themselves, 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. Another threat could be that traitors may be able to store the messages or send them to enemy nodes for cryptanalysis. Using

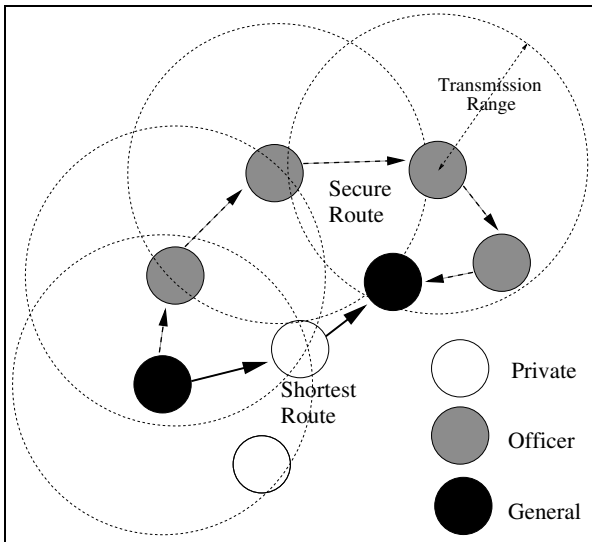


Figure 1: Security-aware Routing - Motivation

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 Figure 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.

3. SECURITY AWARE AD HOC ROUTING

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. 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[4, 6] routing protocols, and more recently, on augmentations that exploit additional information available on the ad-hoc nodes[13, 7] 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. However, the protocol metric is still the length of the routes, measured typically as hop-count. In this paper, we contend 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.

3.1 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 (RPF or Reverse Path Forwarding).

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[6] as our platform to implement SAR.

3.2 Protocol Metrics

SAR provides applications the ability to incorporate explicit trust levels into the route discovery process. A simple way of incorporating trust levels into ad hoc networks is to mirror existing organizational hierarchies, and associate a value with each privilege level. These values 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.

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 [10]. 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 shown in Table 1. Each of these desirable properties has a cost and

Table 1: 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

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. 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.

4. PROTECTION

In this section 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.

4.1 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 (AAA or Authentication, Authorization and Accounting). 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, techniques for key sharing, and techniques for key agreement between multiple cooperating entities in dynamic collaborative groups 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 [3], 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).

4.2 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 [5]. Threats to information in transit include[5, 12]:

- **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.
- **Interception and Subversion:** Routing protocol traffic and control 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.

5. IMPLEMENTATION

In this section, we describe an implementation of SAR, built as an augmentation to the AODV protocol in the NS-2 [1] 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.

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.

We ran our simulation for different security attributes, packet formats, traffic patterns, and trust hierarchies. Our preliminary results showed 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 messages is higher in SAODV, the performance impact is sustainable.

6. 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.

7. REFERENCES

- [1] The Network Simulator - NS-2. <http://www.isi.edu/nsnam/ns/>.
- [2] E. M. Royer and C-K Toh. A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. *IEEE Personal Communications*, Apr. 1999.
- [3] 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.
- [4] J. Broch and D. B. Johnson. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. IETF Internet Draft, October 1999.
- [5] J. Howard. *An Analysis Of Security Incidents On The Internet 1989 - 1995*. PhD thesis, Doctor of Philosophy in Engineering and Public Policy, Carnegie Mellon University, Apr. 1997.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] S. Murphy and M. Badger and B. Wellington. OSPF with Digital Signatures. RFC 2154.
- [10] B. Smith, S. Murthy, and J. Garcia-Luna-Aceves. Securing the Border Gateway Routing Protocols. In *Global Internet '96*, London, UK, Nov. 1996.
- [11] 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.
- [12] W. Stallings. *Network and Internetwork Security Principles and Practice*. Prentice Hall, Englewood Cliffs, NJ, 1995.
- [13] 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.
- [14] 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.