2-2008

Adaptive Threat Modeling for Secure Ad Hoc Routing Protocols

Todd R. Andel
Air Force Institute of Technology

Alec Yasinsac

Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Electronic Notes in Theoretical Computer Science 197 (2008) 3–14
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Adaptive Threat Modeling for Secure Ad Hoc Routing Protocols

Todd R. Andel[1,3]

Department of Electrical and Computer Engineering
Air Force Institute of Tehcnology
Wright-Patterson AFB, OH, USA

Alec Yasinsac[2,4]

Department of Computer Science
Florida State University
Tallahassee, FL, USA

Abstract

Secure routing protocols for mobile ad hoc networks provide the required functionality for proper network operation. If the underlying routing protocol cannot be trusted to follow the protocol operations, additional trust layers, such as authentication, cannot be obtained. Threat models drive analysis capabilities, affecting how we evaluate trust. Current attacker threat models limit the results obtained during protocol security analysis over ad hoc routing protocols. Developing a proper threat model to evaluate security properties in mobile ad hoc routing protocols presents a significant challenge. If the attacker strength is too weak, we miss vital security flaws. If the attacker strength is too strong, we cannot identify the minimum required attacker capabilities needed to break the routing protocol. In this paper we present an adaptive threat model to evaluate route discovery attacks against ad hoc routing protocols. Our approach enables us to evaluate trust in the ad hoc routing process and allows us to identify minimum requirements an attacker needs to break a given routing protocol.

Keywords: Mobile ad hoc networks, secure routing, security analysis, threat modeling.

1 Introduction

Mobile ad hoc networks (MANETs) consist of portable wireless nodes that do not use predetermined communication infrastructure. Each node in a MANET implementation can operate as source, destination, or intermediate router. Ad hoc rout-

[1] The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

[2] Alec Yasinsac is in part supported by U.S. Army Research Laboratory and the U.S. Army Research Office under grant W91NF-04-1-0415

[3] Email: todd.andel@afit.edu

[4] Email: yasinsac@cs.fsu.edu

doi:10.1016/j.entcs.2007.12.013

ing protocols provide the functionality necessary for wireless nodes to communicate with nodes outside their local transmission range. Ad hoc routing protocols [3,14] commonly utilize two-phased routing approaches, in which a route is first determined using a route discovery phase and data is then forwarded between a given source-destination pair over the identified route.

In order for MANET routing protocols to function as desired, we must trust that intermediate nodes within the routing path follow the protocol rules. Trusting intermediate nodes to follow the protocol rules is a significant issue in MANETs, as these networks consist of highly dynamic nodes. Nodes may join or leave the network and network topology changes with mobility.

Developing a proper threat model against MANET routing protocols presents a significant challenge. Defining a threat model is directly related to applying assumptions to attacker capabilities. The attacker strength may range from assuming the attacker has the same power and capability of a non-malicious node to assuming the attacker has virtually no limitations, [5] as viewed in the classical Dolev-Yao [7] attacker model.

In this paper we propose an adaptive threat model to analyze attacks against the route discovery phase in MANET routing protocols. By using an adaptive threat model, we can identify the minimum attacker capabilities required to break a given routing protocol. This approach is different than the traditional approach that limits, or bounds, the analysis results by placing restrictions on the attacker. In the traditional approach, authors tend to claim protocol security based on a fixed environment. However, the security results are only applicable if analyzed within the author's assumptions on the attacker capabilities. These *secure* routing protocols may not be secure outside of the respective assumptions. For instance, work in [3] lists many proposed security solutions along with their operational requirements and drawbacks. Inconsistent operational and security requirements result in claimed secure routing protocols that have flaws and are vulnerable to attacks. Additionally, it is infeasible to compare multiple protocols without common assumptions or security definitions. Our adaptive threat model does not pose the same artificial limitations resulting from bounded security evaluations based on author assumptions. The adaptive threat model is intended to analyze MANET routing protocols for the existence of vulnerabilities, not the absence of such under an author's stated limitations. Since we do not fix the attacker capabilities, our technique allows for a common or baseline comparison between multiple protocols. Adaptive threat models allows us to effectively analyze the ability to trust intermediate nodes to follow the routing protocol rules.

In the remainder of this paper we discuss attack sources, the canonical approach to MANET threat modeling, and identify the limitations faced by existing threat models. We continue with our major contribution in the proposed adaptive MANET threat model and provide our conclusions.

[5] With the exception of breaking cryptographic primitives in polynomial time.

2 Attacking Route Discovery

Ad hoc routing protocols face many attacks, to include denial of service, packet delay, packet modification, packet dropping, and others. We focus on attacks against the route discovery phase. Route discovery attackers attempt to corrupt routes to be inconsistent with the current network topology. Secure routes are a core component to the network's overall trust.

2.1 Attack Sources

We consider two attack sources: *outsider* or *insider*.

- *Outsider* attackers do not have trusted keys. They typically rely on message relay, replay, or delay to influence routing protocols.
- *Insider* threats occur when a fully trusted node, with appropriate keying material, is compromised.

Malicious insiders are much more difficult to defend against than malicious outsiders because they hold legitimate keys. Additionally, malicious insiders can generally act as malicious outsiders as well.

2.2 Classical Routing Attacks

There are known classical attacks that occur against all MANET two-phased routing protocols. These attacks include the Sybil attack [6], the invisible node attack [10,13] and routing wormholes [8].

In a Sybil attack, multiple compromised nodes share keying material and can operate as multiple identities during route discovery. When a Sybil attacker claims another identity during route discovery, the resulting route does not reflect the given network topology. The attacker is not bound to continue to perform as the forged identity during the subsequent data communication over the discovered route.

The invisible node attack (INA) occurs when a node participates in a routing protocol without revealing its identity. An invisible node simply forwards messages between the source and destination during route discovery, regardless if keying material is being utilized or not. Any discovered route that is dependent on the invisible node reports a path that does not reflect the current network topology.

Routing wormholes utilize two nodes to create a tunnel or special out-of-band network to either make a route appear shorter than it is or to completely hide one wormhole endpoint.

While there have been numerous attempts to solve these attacks [8,10,11,13,16] no solution provides a guaranteed defense [2]. The core element enabling these attacks is the inability to positively identify ones' neighbors. Without proper identification capabilities, it is impossible to trust the identities of nodes we are communicating with, to include the intermediate nodes making up the routing path.

In addition to these classical attacks, we must also evaluate MANET routing protocols to determine if the protocol messages themselves allow an attacker to cor-

rupt the route discovery process, subsequently affecting the network trust. Adaptive threat modeling allows us to evaluate route corruption attempts and identify attacker capabilities under which a protocol may fail.

3 Canonical Threat Modeling

Modeling attacker capabilities poses a significant challenge for proper MANET protocol security analysis. In the *security protocol* community, the Dolev-Yao [7] model provides the strongest formal model to effectively evaluate authentication [6] protocols. In the *secure routing* community, the attacker model does not traditionally follow formalized attacker models.

3.1 The Dolev-Yao Attacker

The Dolev-Yao model is the traditional approach to formally model attackers against authentication protocols. The authors define the attacker as: "someone who first taps the communication line to obtain messages and then tries everything he can to discover the [shared secret]" [7]. They additionally provide the following attacker assumptions:

- The attacker hears all messages.
- The attacker is a trusted user and can initiate communication to any node.
- The attacker can be the communication target for any node.

The Dolev-Yao attacker model also assumes perfect cryptography. That is, it assumes all cryptographic mechanisms are perfectly secure and brute force key enumeration attacks cannot be performed in polynomial time.

During analysis, the Dolev-Yao attacker uses information obtained from captured messages to replay, modify, or create new messages, in order to access unauthorized secret information. Formal analysis techniques to evaluate authentication protocols commonly model the initiator and target nodes as endpoints and channel all communication through a centralized Dolev-Yao attacker [15], as illustrated in Fig. 1a.

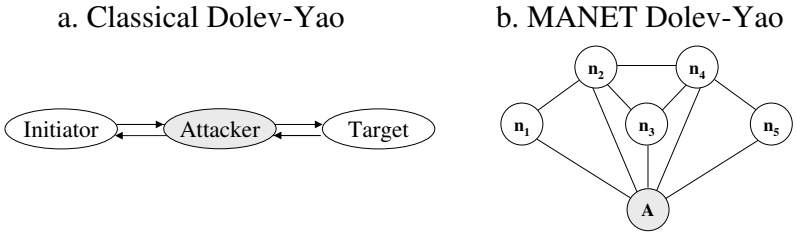

Fig. 1. Dolev-Yao Attacker

[6] Authentication protocols are commonly referred to as cryptographic protocols, not to be confused with secure routing protocols.

Since the intermediate nodes comprising the physical path are irrelevant to the end-to-end authentication security requirement, the attacker is modeled as the communication channel between the initiator and target. The modeled attacker simply relays all messages between the initiator-target pair until it accumulates the information required to inject messages and break the protocol. The attacker can replace any message, since message deliverability between an initiator-target pair cannot be guaranteed in a distributed environment. Since the attacker captures all messages, it can build its knowledge base over extracted information, such as a session key or nonce.[7] When evaluating authentication protocols with a centralized attacker, one must remind themselves they are not modeling the physical communication hops, but modeling an end-to-end message abstraction.

3.2 MANET Attacker Models

While the Dolev-Yao approach provides an effective means to formally model attacks against authentication protocols, modeling attacks against MANET routing protocols poses a different requirement.

An *authentication (or cryptographic) protocol's* goal is generally to share a secret between an authenticated source and destination. The Dolev-Yao approach effectively encapsulates attacks against an authentication protocol's end-to-end security requirement. As Fig. 1a indicates, the end-to-end security requirement does not consider intermediate nodes within the communication path. Authentication protocol security evaluations usually do not consider attacks against the path between the initiator-target pair.

On the other hand, MANET *secure routing protocols* must ensure the route discovery process delivers routes that reflect the current network topology. The actions taken by the intermediate nodes making up the route are significant and cannot be abstracted out of the formal model during security evaluations over the route discovery process. In the context of secure ad hoc routing protocols, the Dolev-Yao attacker can be viewed according to Fig. 1b, where the attacker has a communication link to all network nodes.

The Dolev-Yao attacker in a MANET environment can capture any message in the network and can transmit a message to any network node. Since the attacker can effectively reduce communication between any two nodes to a two-hop network channeled through the attacker, the Dolev-Yao attacker provides the strongest attacker model for evaluating MANET routing protocols. If a routing protocol can be shown secure against a Dolev-Yao attacker, the protocol will be secure against any attacker capability.

Unfortunately, the Dolev-Yao model is not traditionally used to evaluate MANET routing protocols. The most common approach to model attacker capabilities used throughout the MANET community is to assume the attacker node has the same capabilities as any node within the network. Forcing an attacker to use nodes without any additional capability unrealistically limits the attacker. Re-

[7] A nonce is a random number used once in an authentication protocol instance.

sults from a limited attacker evaluation may claim security that can be subverted by changing the attacker restrictions. Fortunately, there have been some recent efforts to more formally model the attacker.

Active-n-m Attacker. Work in [9] presents a formalized attacker model as *active-n-m*, where n is the number of compromised insiders that hold keying material, and m is the total number of attacker nodes in the network. All attacker nodes in the *active-n-m* approach have the same capabilities as non-malicious nodes, plus the nodes have the ability to distribute compromised keys to all other *m-1* attackers.

The authors in [1] utilize the *active-n-m* approach with an additional configuration limitation. They combine all neighboring attackers that can share information from captured messages during network operation into a single node. The combined single attacker is therefore limited in its transmission capability from a single node location, effectively changing the network topology. Forcing two attackers that can communicate with one another to be represented as a single entity may overly restrict attacker capabilities. The two nodes are now modeled to act as a single transmission point, which is not representative of the true network topology. This approach is inappropriate, since non-malicious nodes cannot assume the attackers will cooperate as a single entity to provide a path during route discovery.

Parmetric Attacker. The *parametric attacker* approach in [12] further refines the *active-n-m* attacker. The parametric attacker, represented by *A(k, SA)*, identifies the number of attacker nodes k and the initial pre-distributed attacker knowledge S_A, such as keys. The Dolev-Yao attacker is included as a special boundary case, in which each network link contains a parametric attacker. However, the authors do not indicate how the Dolev-Yao boundary case interacts with the protocol. Additionally, the authors do not allow colluding attackers to share captured information during network operation. The scenarios they evaluate contain a single adversary with the same communication capabilities exhibited by the non-malicious nodes.

Both the *active-n-m* and the non-boundary case *parametric attacker* are scenario dependent. That is, security analysis results using these attacker models vary, depending on network configuration, and the location and number of attacker nodes. Attacks may be overlooked if analyzed in the wrong topology.

4 An Adaptive Threat Model

In our modeling approach, we wish to maintain Dolev-Yao attacker strength to determine if the route discovery process can *possibly* be violated. That is, can a route be returned that is not consistent with the current network topology? It is important to focus on *possible* route violations instead of *probable* attacks based on network configurations, number of attackers, or attacker strength, since we are interested in determining if routing attacks exist against a given protocol. If a protocol is secure against the Dolev-Yao attacker it will provide security against all attackers.

While the Dolev-Yao attacker provides the strongest modeling approach, mod-

eling the strongest attacker does not provide the precision to identify the minimum capabilities required to break a protocol. Understanding the minimum capabilities required to break a routing protocol provides significant understanding into what expected environments the protocol can successfully find trusted routes.

Assuming that the attacker cannot break cryptographic primitives in polynomial time, the attacker capability, or strength, is determined by:

- The attacker's communication capability.
- Whether the attacker is an insider or an outsider.
- Whether a single or multiple attackers exist.

The attacker communication range and ability to share information with other attackers relate to the attacker's ability to *learn* information required to break a protocol. The attacker's status as an insider vs. an outsider determines what type of messages the attacker can generate.

Our adaptive modeling approach attempts to identify the minimum attacker strengths required to corrupt routes returned by the route discovery phase. This approach follows work in [5] to look beyond the capabilities provided by the Dolev-Yao model during authentication protocol analysis and evaluate different attacker environments in ubiquitous systems. Adapting the attacker capabilities allow us to identify the conditions in which an attack is successful and does not suffer from limitations imposed by restricting the attacker. At the same time, including the Dolev-Yao attacker ensures that attacks missed by a weaker attacker due to network configurations can still be discovered.

4.1 The Model

We offer the attacker classification shown in Fig. 2, tailored specifically to search for route integrity attacks against MANET routing protocols. Route integrity attacks corrupt the route discovery process, resulting in returned paths that do not exist for the given network topology. Analysis using the adaptive attacker views the mobile network as a snapshot in time, since valid routes that fail due to node movement are not malicious. Our adaptive attacker classification allows the security analyst the ability to identify capabilities required to break a routing protocol. Evaluating a protocol against the spectrum of attacker capabilities provides a more complete security analysis outcome, as opposed to claiming security based on a restricted attacker that may be easily subverted by an unlimited adversary or under different operational scenarios.

Within our attacker classification, an outsider node has the capability to capture any messages transmitted within its reception range, can replay any messages it has captured, and can create messages from information it has recovered from original knowledge or captured messages. The attacker's goal is to return a route that is not consistent with the current network topology. The intended effects depend on whether the attacker is an outsider or a trusted insider.

The malicious outsider's goals are to either corrupt the route so that an invalid

Attacker Strength	Communication Capability	Insider/ Outsider	Attacker Category	Attacker Goal on Route Integrity
Single Intruder	• Same as non-malicious node	Outsider	I	• Add self to route • Corrupt route
		Insider	II	• Corrupt route
	• Unlimited receive radius • Transmission radius same as non-malicious node	Outsider	III	• Add self to route • Corrupt route
		Insider	IV	• Corrupt route
	• No limitations (Dolev-Yao)	Outsider	V	• Add self to route • Corrupt route
		Insider	VI	• Corrupt route
Multiple Intruders (all intruder keys shared)	• Same as non-malicious node	Insider	VII	• Corrupt route
	• Unlimited receive radius • Transmission radius same as non-malicious node	Insider	VIII	• Corrupt route
	• No limitations (Dolev-Yao)	Insider	IX	• Corrupt route

Fig. 2. Attacker Classification

path from the source to the destination exists or to add itself to the route, since it is not an authorized user. Insider nodes have the added capability to sign messages, as they hold a trusted cryptographic key. Since malicious insiders are authorized users, adding themselves to a valid route does not constitute an attack for the malicious insider. Therefore, malicious insiders only attempt to corrupt the route.

In order to identify the required attacker strength to break a protocol, our attacker classification looks at both single intruders and multiple intruders, along with various communication capabilities an attacker may have. The attacker capabilities range from having the same capabilities as a standard node in the network to having no transmission or reception limitations, as modeled with Dolev-Yao capabilities. We further refine the Dolev-Yao attacker by allowing the attacker to be an outsider or an insider. The canonical Dolev-Yao model assumes the attacker is a trusted insider. We refine the attacker to determine if an attacker without communication limitations has different effects based on whether the adversary has trusted keys or not.

Between the standard node attacker and the Dolev-Yao extremes, we add an attacker with an unlimited reception capability and a limited transmission capability. This category (classifications III, IV, and VIII) does not assume the attacker node follows bi-directional communication rules (i.e., the attacker is asymmetrical), allowing the attacker to appear as a normal node during transmissions, while at the same time allowing any message to be received. An attacker with this capability can arise by having a more powerful transceiver or antenna than the standard network nodes. However, the attacker can restrict its transmission range by adjusting its output power.

We illustrate the asymmetrical attacker in Fig. 3. The attacker can capture any message in the network, allowing it to craft routing attacks if it obtains enabling information. Since the attacker restricts its transmission to nodes S and D, nodes n_1 and n_2 are unaware that a forward link exists to node A. If node A obtains the correct information, the attacker may be able to remove node n_1 from the path S-n_1-n_2-D, resulting in the corrupt path S-n_2-D. We provide an example attack in

Section 4.2.

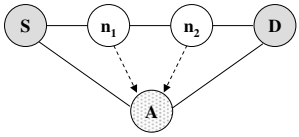

Fig. 3. Asymmetric Attacker

We can also use the unlimited reception range to abstract out any special network topology configurations that may help enable an attack. By enabling an attacker to receive all network traffic, we inherently consider any network topology, attacker position, or additional capabilities provided by collusion between individual attacker nodes. Therefore, we do not lose any capabilities over the existing *active-n-m* approach. For instance, work in [1,4] uses the *active-n-m* approach to provide attacks against the Ariadne [9] protocol. These attacks are based on various network configurations, including some instances using colluding nodes. All configurations and collusion scenarios simply allow the attacker the ability to *hear* information that it can then use to create a corrupted routing message. Our unlimited receive capability option does not require crafty scenarios to receive the correct enabling information, since all publicly transmitted messages have already been captured.

For multiple intruders, we assume the attackers are always colluding insiders. We implicitly include multiple outsider attackers since the outsiders have no cryptographic keys to share and the *no-limitation* outsider option (classification V) allows a single node to receive all information in the network and to direct transmission to any point in the network. We assume that all malicious insiders collude, since multiple attackers that do not work together do not have any greater capability to corrupt the route discovery process than a single attacker, although network performance may be affected. If the attackers follow the standard node capability (classification VII) and are not within each other's transmission range, we permit the colluding nodes to at least share cryptographic keys, allowing us to search for attacks enabled by the ability for a single node to sign or decrypt information computed with the colluding attacker's key.

When we allow an unlimited receive radius in a multiple colluding attacker environment, we allow the nodes to share captured information by hearing the same messages obtained during protocol operation, regardless of the network configuration. Sharing information in our model through this mechanism has the same effect as multiple colluders setting up a secret out-of-band communication mechanism or having many intermediate colluding nodes that simply relay information between two malicious attackers.

The adaptive model takes into account any possible network path. Since we cannot ensure every routing packet is delivered in a wireless networking environment, we must allow the possibility for any node, or message event sequence, to interact within one protocol round. [8] That is, if it is possible for an attacker node to break a

[8] A route discovery round is a complete route discovery process initiated by one source to find a path to the source's desired destination.

protocol round, regardless if a non-malicious node has already processed a message for that sequence number received from a shorter route, the routing protocol is not secure since we cannot ensure another route has already been processed. Again, we are evaluating the routing protocol for *possible* attacks, not *probable* attacks.

4.2 An Example

Let us consider an example using our attacker classification for a single insider attacker (classifications II, IV and VI). We evaluate signature-based Ariadne [9] against the topology in Fig. 4.

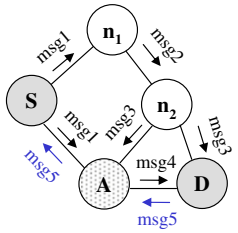

Fig. 4. Example Single Attacker Topology

During the route request (rreq), each intermediate node adds itself to the route path, calculates a hash value, produces a signature over the new packet, and broadcasts a message containing the new path, new hash value, and appended signature. For example, *msg2* is constructed as:

$$msg2 = (rreq, S, D, h_{n1}, (n_1)), (sig_{n1}),$$

where the hash value h_{n1} is computed by the one-way hash function H as $h_{n1} = H(n_1, h_s)$ and h_s is a shared secret between S and D.

In the example scenario, node S attempts to set up a route to node D, with node A being a malicious insider. The possible routes according the topology are S-A-D, S-A-n_2-D, S-n_1-n_2-D, and S-n_1-n_2-A-D.

We do not consider *A's* ability to drop packets once a route is set up or *A's* ability to simply relay messages (i.e., the invisible node attack), since we have already determined these attacks exist. Here we are searching for attacks enabled by information revealed by the protocol messages. Therefore, we search for *A's* ability to trick the protocol into accepting the invalid path S-n_1-A-D or S-n_2-A-D.

Using the attacker category II, the adversary has the same capability as all other nodes in the network. When A receives *msg3* from n_2, it removes n_2 from the path and n_2*'s* signature. The per-hop, one-way hash value h_{n2} is intended to guard against A taking this action, but node A can compute n_1*'s* hash embedded into *msg2* directly from *msg1*, since $h_{n1} = H(n_1, h_s)$. The destination node D validates the hash value and signatures, accepting the path S-n_1-A-D, which does not exist. Node D then creates a signed route reply (rrep) in *msg5*, through A to node S. The complete message transmission for the attack follows, with **msg4* introducing the malicious path:

$$msg1 = (rreq, S, D, h_s()), (sig_s)$$

$$msg2 = (rreq, S, D, h_{n1}, (n_1)), (sig_s, sig_{n1})$$
$$msg3 = (rreq, S, D, h_{n2}, (n_1, n_2)), (sig_s, sig_{n1}, sig_{n2})$$
$$*msg4 = (rreq, S, D, h_A, (n_1, A)), (sig_s, sig_{n1}, sig_A)$$
$$\text{where } h_A = H(A, h_{n1}) = H(A, H(n_1, h_s))$$
$$msg5 = (rrep, S, D, (n_1, A)), (sig_D).$$

This attack is the same attack presented in [4]. However, the attack depends on the network topology. In order for this attack to be possible, node A must be able to receive *msg1*, *msg3*, and *msg5*, and be able to transmit *msg4* to D and relay *msg5* to S. Consider what would happen if the link between n_2 and A did not exist. Node A would never recover sig_{n1} from *msg3*. We can create the same attack if we allow A the ability to receive all messages. If A has an unlimited receive capability (category IV), it can extract n_1*'s* signature and hash value directly from *msg2*, resulting in the ability to create the same corrupted path S-n_1-A-D. However, we still require the ability to send and receive messages between S and D.

Our final classification for the single malicious insider (category VI) provides no restrictions as the full Dolev-Yao model, which imposes no topology requirements to duplicate the previous attack. The Dolev-Yao attacker acts as a fail-safe in case the previous categories failed to discover an attacker due to the network topology that was evaluated. However, exclusively using the Dolev-Yao model would not have allowed us the ability to identify the minimum attacker capabilities required to break the protocol.

As the example indicates, the category II attacker utilizing standard node capabilities depends on the network topology chosen for the evaluation. To ensure this attack is found during evaluation against a category II attacker, all network configurations need to be considered. Topology dependent attacks challenge the security analyst to a grueling manual evaluation process to evaluate all possible network configurations. Our adaptive threat model provides the attacker strength of the Dolev-Yao attacker to discover if an attack is possible in any topology and provides the precision to identify minimum attacker capabilities if evaluated within an enabling network topology.

5 Conclusion

In this paper we discussed the various attacker threat models being used to evaluate the MANET route discovery process. We saw how the current threat models may overly restrict the attacker's capabilities, resulting in claimed secure routing protocols that may actually be easily attacked, due the fact that we cannot assume an attacker will follow the restrictions assumed by the analyst.

Our contribution provides an adaptive threat model for MANET security evaluations. Instead of claiming protocol security based on attacker assumptions, we adapt the attacker capabilities in order to determine at what point a protocol may fail. By adjusting the attacker communication capabilities, we do not rely on special network topologies to enable attacks. Our model presents us with a difficult challenge. We now have many different attack scenarios that we must evaluate. For

instance, the attacker model presented in Fig. 2 requires the security analyst to analyze nine different scenarios to provide a complete analysis picture. This analysis requirement drives research into automated analysis techniques.

While we have presented a handful of possible ad hoc routing attacks, we contend that any attack against the ad hoc route discovery phase could be represented and discovered utilizing our adaptive attacker classification. Our adaptive model ensures attackers are discovered via the unrestricted Dolev-Yao attacker, while at the same time provides the precision to investigate minimum capabilities (communication limits, trusted insider or outsider, single or multiple attackers) required to corrupt MANET routing protocols.

Until MANET routing protocols can be secured and properly evaluated, ultimate network trust cannot be achieved.

References

[1] Ács, G., L. Buttyán, and I. Vajda, *Provably secure on-demand source routing in mobile ad hoc networks*, IEEE Transactions on Mobile Computing. **5** (2006), 1533-1546

[2] Andel, T.R. and A. Yasinsac, *The Invisible Node Attack Revisited*, Proc. 2007 IEEE SoutheastCon. (2007), 686-691.

[3] Argyroudis, P.G., and D. O'Mahony, *Secure routing for mobile ad hoc networks*, IEEE Communications Surveys & Tutorials. **7** (2005), 2-21.

[4] Buttyán, L. and I. Vajda, *Towards provable security for ad hoc routing protocols*. Proc. 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. (2004), 94-105.

[5] Creese, S., M. Goldsmith, B. Roscoe, and I. Zakiuddin, *The Attacker in Ubiquitous Computing Environments: Formalising the Threat Model*, Proc. 1st Intl Workshop on Formal Aspects in Security and Trust. (2003), 83-97.

[6] Douceur, J.R., *The Sybil attack*, Proc. 1st Intl. Workshop on Peer-to-Peer Sys. (2002).

[7] Dolev, D., and A. Yao, *On the security of public key protocols*, IEEE Transactions on Information Theory. **29** (1983), 198-208.

[8] Hu, Y.C., A. Perrig, and D.B. Johnson, *Packet leashes: a defense against wormhole attacks in wireless networks*, Proc. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. (2003), 1976-1986.

[9] Hu, Y.C., A. Perrig, and D.B. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Wireless Networks. **11** (2005), 21-38.

[10] Marshall, J., V. Thakur, and A. Yasinsac, *Identifying flaws in the secure routing protocol*, Proc. 2003 IEEE International Performance, Computing, and Communications Conference. (2003), 167-174.

[11] Marti, S., T.J. Giuli, K. Lai, and M. Baker, *Mitigating routing misbehavior in mobile ad hoc networks*, Proc. Annual International Conference on Mobile Computing and Networking. (2000), 255-265.

[12] Nanz, S., "Specification and Security Analysis of Mobile Ad-Hoc Networks," P.hD. thesis, Imperial College, London, 2006.

[13] Ramachandran, P. and A. Yasinsac, *Limitations of on demand secure routing protocols*, Proc. Fifth Annual IEEE SMC Information Assurance Workshop. (2004), 52-59.

[14] Royer, E.M., and C.-K. Toh, *A review of current routing protocols for ad hoc mobile wireless networks*, IEEE Personal Communications. **6** (1999), 46-55.

[15] Ryan, P. and S. Schneider, "Modelling and Analysis of Security Protocols," Addison-Wesley, Harlow, England, 2001.

[16] Suen, T. and A. Yasinsac, *Peer identification in wireless and sensor networks using signal properties*, Proc. 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems Conference. (2005), 826-833.