An Attacker Model for MANET Routing Security

Jared Cordasco
Department of Computer Science
Stevens Institute of Technology
Hoboken, New Jersey, USA
jcordasc@cs.stevens.edu

Susanne Wetzel
Department of Computer Science
Stevens Institute of Technology
Hoboken, New Jersey, USA
swetzel@cs.stevens.edu

ABSTRACT

Mobile ad-hoc networks are becoming ever more popular due to their flexibility, low cost, and ease of deployment. However, to achieve these benefits the network must employ a sophisticated routing protocol. Early proposed routing protocols were not designed to operate in the presence of attackers. There have been many subsequent attempts to secure these protocols, each with its own advantages and disadvantages. To allow for a comparison of these secure protocols, a single common attacker model is needed. Our first contribution in this work is to develop a comprehensive attacker model categorizing attackers based on their capabilities. This is in contrast to the existing models which seek to categorize attacks and then map that categorization back onto the attackers. Our second contribution is an analysis of the SAODV routing protocol using our new model, which demonstrates the structured approach inherent in our model and its benefits compared to existing work.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and Protection*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless Communication*

General Terms

Design, Reliability, Security

Keywords

MANET, ad-hoc, routing, security, attacker model

1. INTRODUCTION

Mobile ad-hoc networks (MANETs) allow for wireless devices to form a network without the need for central infrastructure. While the lack of need for infrastructure allows the network to be very flexible, it also makes routing a critical concern in the network. The original proposals for MANET routing such as DSR[13], DSDV[17], and AODV[18] did not take security into consideration. As a result, many attacks have been found which can disrupt the functioning of a MANET. Subsequent protocol proposals were designed to address one or more of these attacks [3, 9, 11, 16, 19, 20, 22], yet no protocol has proven secure against all attackers [2].

In order to allow for an accurate comparison of the security properties of these proposals, a common attacker model is necessary which allows for proper evaluation. Unfortunately, no suitable model has yet been developed. Instead, authors analyze their protocol in a scenario of their choice with restrictions designed to ease their proof of security [10, 11, 14, 21]. These models are typically developed by looking at the attack or attacks under consideration and trying to categorize attackers based on the characteristics of these attacks while placing topological restrictions on the network. Due to this, unforeseen vulnerabilities can arise when the protocol is applied to real-world scenarios that cannot be molded to fit the topological constraints. In addition to bordering on contrived, each model uses a different set of restrictions, considers different topologies, or addresses different attacks. This makes accurate comparison of protocols and their security properties impossible.

In contrast, developing models starting from the attackers' capabilities removes the topological constraints and the resultant overlooked networks that can present a new vulnerability. In fact, working from attacker capabilities to attacks is not only topology-agnostic, but also protocol-agnostic. In addition, once attackers are categorized by their capabilities, specific attacks can be mapped to the categories of attackers with sufficient capabilities to perform such attacks. Similarly, the necessary capabilities for performing a specific attack can be determined by comparing categories of attackers that can and cannot perform the attack.

In this work, we use this alternative approach to develop a novel attacker model focusing on categorizing attacker capabilities. To the best of our knowledge, this is the first attacker model of this form for MANET routing. Our new model allows for simplified determination of necessary and sufficient capabilities for performing specific attacks. In addition, due to the complete coverage of our model, real-world scenarios are included in the analysis, ensuring that vulnerabilities will be found during analysis and thus before deployment. Our proposed model is both topology- and protocol-agnostic. As such it allows for comparison of various protocols in one common model. Finally, the ability to

WiSec'09, March 16–18, 2009, Zurich, Switzerland.

combine our model with BAN logic [5], or other formalization frameworks [7], allows for a structured, comprehensive analysis of protocol security. In addition to our first main contribution of the new attacker model, our second main contribution is an example application of our new model to the SAODV protocol, showing how our structured approach exposes a serious, though previously known[1], vulnerability automatically during analysis.

Outline: In Section 2 we first discuss existing attacker models and their attack-based approach. Then, we focus on our first contribution, a new attacker model developed with the capabilities-based approach. We detail the attacker's communication and computation capabilities as well as the application of our model. Section 3 is our second main contribution, an example application of our model to analyze the security mechanism of hash chains as used in the SAODV routing protocol. Finally, Section 4 concludes the paper with a discussion of future work.

2. ATTACKER MODELS

2.1 Existing Models

To date, the analysis of proposed secure routing protocols has taken place under a disparate set of models that vary based on restrictions, topologies, and considered attacks. Most of these models were not proposed for general use, but instead were included in the protocol exposition merely to prove the security of the protocol in some specific scenario [10, 14, 19, 21]. These existing models have concentrated on the attacks and sought to categorize the attacks based on their similarities. This categorization is then transfered onto the attackers to form an attacker model. However, working in this direction does not completely categorize all attackers. In addition, new attacks may require adjustments to the attack categorization which must then be translated to changes in the attacker categorization (Figure 1).

The lack of a common attacker model has made the protocols difficult to compare. Such difficulty can be seen in the lists of operational requirements and drawbacks for each of the proposed solutions surveyed by Argyroudis et al. in [2]. In addition, the real-world networks are often difficult to fit within the topological constraints of these models, and thus vulnerabilities arise that were not considered during the protocol analysis. This is a result of taking a categorization of attacks against which the protocol is supposed to be secure and mapping that back into a categorization of the attackers.

To address the lack of a common attacker model, Hu et al. develop the active $n-m$ attacker model in [11], which they also use to argue the security of their Ariadne protocol. In this model, n is the number of compromised nodes with key material and m is the total number of attackers. All attackers are assumed to be equivalent to compromised nodes. The key limitation of the active $n-m$ model is its topology dependence. Nanz extends the active $n-m$ attacker in [15] to develop the parametric attacker. Unfortunately, this proposal suffers the same flaw. The authors of [1, 6] show the importance of a topology independent approach by using the active $n-m$ attacker in an altered network scenario to attack the Ariadne protocol.

[1]but not discovered in this manner

2.2 Our New Model

An alternative to the existing models is to focus on forming a categorization based on the attacker's capabilities and then place attacks into categories based on the minimum required capabilities for performing the specific attack. This approach has a number of advantages. First, since this method directly categorizes the attackers, the coverage will be complete. Second, due to the fact that every attack has some minimum required attacker capabilities, all existing and future attacks can be matched to an attacker category without adjusting the categorization (Figure 2). Third, our breakdown of attacker capabilities produces a model similar to the Dolev-Yao model [8][2], allowing results under that model to be applied to ad-hoc networks.

In the following, we make use of this alternate approach to develop our new attacker model. While this may appear to be logical and even obvious, to the best of our knowledge, we are the first to use this approach. In the following sections, we detail our model focusing on the two key capabilities that are possessed by every device, both participant and attacker. These two capabilities are communication and computation. We then show how powerful this approach is by analyzing the SAODV protocol and deriving a major vulnerability.

2.2.1 Communication

The attacker's communication capability can be broken down into *send* and *receive* capabilities. Each of these fall into one of three categories.

Category 1 communication is on par with that of an ordinary node in an ad-hoc network. This could be an attacking device using equivalent hardware to that used by nodes in the network. Alternatively, it could be a compromised node. The difference between these two scenarios is the possible possession of key material discussed later.

Category 2 communication is on par with several ordinary nodes (i.e., a number of colluding attackers with capabilities in Category 1).

Category 3 communication allows the node in question to communicate with the entire network. This would be the MANET equivalent to the network-wide Dolev-Yao communication model [8].

In order to explore the combination of these categories when applied to send and receive capabilities, we must first consider an attacker's exposure to detection in each category. Since we are in a wireless medium, reception of communication is a passive action. Therefore, it is difficult for an intrusion detection system (IDS) or other "watchdog" mechanism to differentiate between a device listening to messages within a typical radio range and a device listening to messages from the entire network [4]. Due to this, we assume that if the attacker has the capability, it will choose to listen to the entire network.

Sending messages is different from receiving in that it is an active operation. There have been several proposals for

[2]Dolev-Yao is a model in which the attacker has full send/receive capabilities (i.e., control over the transmission medium). Our model creates subsections of the network in which attackers display Dolev-Yao type control.

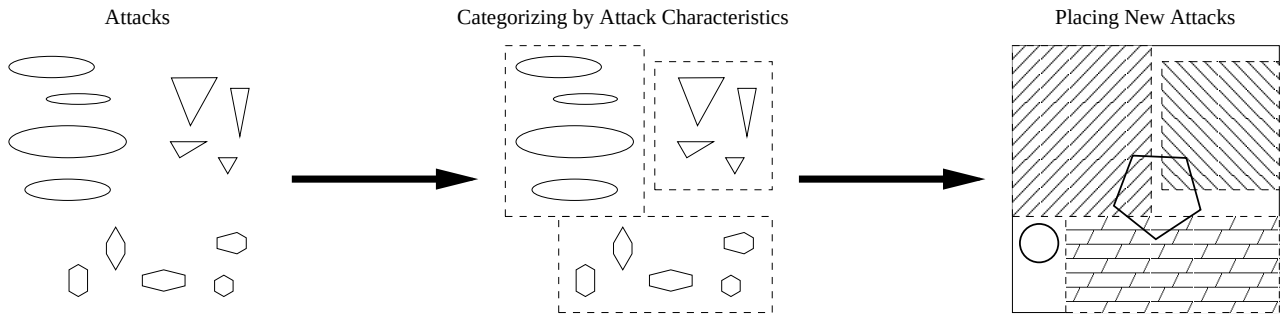

Figure 1: Categorizing attacks by their characteristics leads to incomplete coverage of the attack space. Meanwhile, new attacks may not clearly fit into any of the existing categories requiring a new categorization.

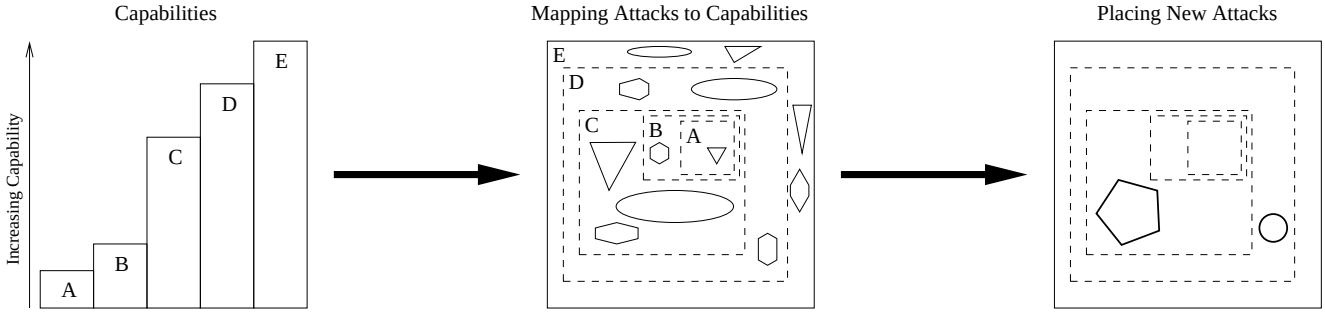

Figure 2: Defining attacker capabilities as increasing subsets (i.e., all capabilities in A are included in sets B through E) allows a clear mapping of attacks to their minimum necessary capabilities. Since every attack has a set of minimum necessary capabilities, all new attacks belong to a unique category.

identifying attackers who are transmitting messages to the entire network using a single identity, or using multiple identities with only a single radio transceiver. Therefore, such transmissions expose the attacker to an increased risk of detection [4]. Thus, it is possible that an attacker with the capability to send messages to the entire network may choose to limit sending messages to nodes within a typical radio range to avoid detection. This situation changes when multiple attackers are colluding. Since there are several radio transceivers and identities, it is possible to avoid detection by existing mechanisms while maintaining a larger portion of the network to which the attackers can transmit.

One final assumption we make concerning an attacker's communication capability is that the transceiver's maximum capabilities are symmetric, however, a device can choose to limit the transceiver's capabilities to avoid detection, if necessary. From this assumption and the passive nature of receiving communications, we propose that an attacker will always use receive capabilities at least equal to its send capabilities. Communication can then be categorized by the following five combinations:

Type I represents an attacker that is using a corrupted node or an equivalent device to launch an attack.

Type	Send Capability	Receive Capability
I	Category 1	Category 1
II	Category 1	Category 3
III	Category 2	Category 2
IV	Category 2	Category 3
V	Category 3	Category 3

Type II represents an attacker using a single device with a more powerful transceiver that allows communication with the entire network, however, the attacker has limited its radio's send capabilities to limit the risk of detection.

Type III is characterized by a number of colluding devices, each of which has communication capabilities equivalent to that of typical node in the network. However, together the devices have a larger sphere of influence.

Type IV is characterized by a number of colluding devices with transceivers that allow communication with the entire network, yet they are limiting their send capabilities to avoid detection.

Finally, *Type V* can be characterized by one or more attackers with powerful transceivers who are not concerned with being detected.

2.2.2 Computation

The computational capabilities of an attacker encompass several different abilities such as decrypting incoming messages, encrypting outgoing messages, and computing secrets. There are two components that affect these abilities: hardware capabilities (pure computation) and available knowledge.

Since computing hardware is advancing at such an accelerated rate, it does not make sense to set performance specifications for the attacker and consider our protocols in such a model. Therefore, since our pure computational power mainly determines which cryptographic methods are secure, we use the model of an almost unlimited attacker whose only restriction is feasibility — a model commonly used in the cryptographic community. Thus, our attacker can only perform operations (without key material) that are feasible in a reasonable amount of time on current hardware. As technology progresses with time, protocols will need to be re-evaluated in this model to determine what information can be considered secure, and whether or not any insecurity can be addressed by increasing bitlength or whether the primitive (and possibly the protocol itself) need to be updated or replaced.

While pure computation may be used to properly decrypt a message or compute a secret, there is an easier way. If the attacker has the private key for an encrypted message, it can decrypt and read the message with little need for any computational sophistication. Therefore, in addition to considering the feasibility of breaking the cryptographic mechanisms employed by a protocol, it is also necessary to evaluate what information is available to the attacker that could allow it to bypass the feasibility limit of the cryptographic mechanism.

The information available to the attacker can come from many different sources. Messages (or parts of messages) that are exchanged unencrypted are one source of information. Furthermore, if an attacker is a valid participant in a network (i.e., an insider), there is some initial knowledge that it will have which possibly includes key material and other parameters. Collusion among several attackers not only increases the attacker's communication capabilities, but it also increases the information available as colluding attackers share all key material, nonces, hash chain seeds, etc. in order to be more powerful. The ability of colluding attackers to acquire more (non-initial) information can also be matched by a single attacker with more sophisticated communication capabilities as described in the previous section. The interplay between the capabilities of an attacker is shown in Figure 3.

Having presented the details of our model we now look at the application of the model, both in general and with a simple example meant to show the power of our approach.

2.2.3 Application of Our New Model

Making use of the newly-proposed attacker model presented in this work requires applying the model to individual protocols and evaluating the results. Our model is independent of the routing mechanisms used and can therefore be applied to evaluate any reactive, proactive, source routed, or distance vector protocol. When the model is applied to a protocol, the protocol specifics dictate a significant portion of the attacker's communication and computational capabilities. The remainder of the attacker's capabilities will be dictated by hardware choices (computation and communication), expected willingness to risk exposure (communication), desired resiliency to collusion, and other such parameters.

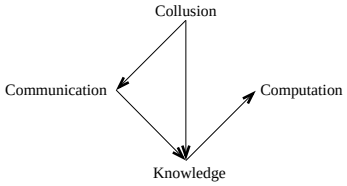

Figure 3: Interplay of attacker capabilities.

To reason about the computational abilities, specifically those enabled by the attacker's knowledge, one can use any of several methodologies ranging from BAN logic [5] to Cremers and Mauw's Operational Semantics [7]. To ease determination of what existing attacks a protocol is vulnerable to, common attacks can be specified by the minimum attacker capabilities necessary to carry out the attack. Then, determining a protocol's vulnerability to existing attacks is as simple as evaluating which capabilities required for the attack are possessed by the attacker.

Expressing existing attack scenarios in this new model requires a change of perspective. Far too often attackers have been modeled in ways that unduly limit their capabilities. These limitations hurt the "big picture" comparisons of protocol vulnerability. In our new model, it is easier to model a more powerful, more general attacker than a highly specific, limited one. The use of this generalized attacker allows for a more thorough analysis. However, if the more limited attacker is desired, it too can be expressed in our model.

For example, suppose there is a desire to model an attacker who eavesdrops in one area of the network, then moves to another area and resumes eavesdropping there. The more general attacker model considers two devices, one in each location, which both eavesdrop and collaborate to attack the protocol. While this attacker is in fact more powerful, it avoids the potential pitfalls involved with poor choices of parameters such as speed of travel, distance between locations, etc. By using the more general model, we have a more thorough analysis that is independent of these parameters.

Another example arises when modeling adaptive node compromise. In this case, the more general model consists of a constant subset of collaborating attackers that includes all nodes compromised over the course of the adaptive attack. (As insiders, all of these nodes contribute their key material to the general attacker knowledge.) Still, a more specific attacker can be modeled, if necessary, by introducing a timestamp to the message representation in the logic being used to argue about knowledge and computation. This in turn requires far more specification, more parameters to be set, etc., but it is possible. The fact that the more general attacker is preferable to model is an additional benefit of our model.

3. EXAMPLE ILLUSTRATING AN ATTACK ON SAODV

The second main contribution of this work is the application of our new model to the SAODV MANET routing protocol. We show how the structured approach, inherent in our model, automatically reveals a critical vulnerability in SAODV. To demonstrate the power of this model, we consider the mechanism used to secure the hop count information. The attack we arrive at through analysis with our model is a known attack for falsely advertising more attractive routes. However, we arrive at the vulnerability through a more structured approach. In addition, because of this approach we see how the analysis of the possible attack leads to statements of vulnerability for hash chains, the SAODV protocol, and more generally any protocol relying on limited dissemination or ordered delivery. Section 3.1 gives and overview of the features of the SAODV protocol necessary for the analysis. Section 3.2 follows with the actual application of our model and the details for deriving the attack.

3.1 SAODV Overview

In [18], Perkins and Royer introduced the Ad-hoc On-demand Distance Vector (AODV) routing protocol. As with the other original MANET routing protocols, it was designed without any inherent security mechanisms. Zapata and Asokan have tried to remedy this by introducing SAODV [22]. Their protocol attempts to prevent impersonation attacks, worm hole and black hole attacks, as well as denial of service attacks. However, to do this, SAODV requires that there is a key management system available that provides public keys for each node in the network.

The SAODV protocol attempts to secure the routing packets with two different mechanisms. This is necessary as there are two different types of data within the routing messages: mutable and immutable data. Rather than using an expensive cryptographic primitive such as digital signatures for the entire message, which would require recomputation at every node, the expensive operations are performed once to secure the immutable data. The mutable data is secured using a less expensive primitive which allows it to be recomputed at every node without creating an unreasonable overhead.

SAODV uses RSA-based digital signatures to secure the immutable portions of the routing message. This includes not only the immutable parts of the original AODV message, but also the immutable parts of the SAODV extension. The only fields not included in this signature are the AODV Hop_Count and SAODV $Hash$ fields. The signature, along with the public key that can be used to verify it, are included in the packet. When a node receives a signed SAODV message, it is required to verify the signature before performing any additional processing. If the signature is verified, then processing proceeds, otherwise the packet is discarded. This mechanism is designed to prevent impersonation attacks.

In order to protect the mutable Hop_Count field of the AODV packet, SAODV uses a one-way hash chain. An initial seed value is generated. This value is then repeatedly hashed Max_Hop_Count times to arrive at the value stored in the Top_Hash field. The seed value is used as the initial value of the $Hash$ field. Formally this means

$$Top\_Hash = h^{Max\_Hop\_Count}(seed)$$

where h is a one-way hash function and $h^i(x)$ is the iterative hashing of x, i times. Upon receiving an SAODV message, the receiving node has to confirm that

$$Top\_Hash \stackrel{?}{=} h^{Max\_Hop\_Count - Hop\_Count}(Hash). \quad (1)$$

It must then increment the Hop_Count field and set $Hash = h(Hash)$. Since a one-way hash function is used, it should be computationally infeasible for a node to determine a value in the hash chain it has not seen, which would correspond to a hop count lower than that specified in the routing message it received.

Securing the hop count is a necessity in order to prevent nodes from falsely advertising the length of a route. Lazy or selfish nodes may seek to exclude themselves from routes in order to conserve their resources for their own use. They can accomplish this by inflating the hop count for the route passing through themselves. While this goes against the cooperative nature of the ad-hoc network, there is a greater threat. The attacker who can advertise a short route to the specified destination can "pull" data towards itself thereby allowing it to eavesdrop or, by carefully choosing which routes to shorten, can perform a covert denial of service attack (DoS) against a node common to all the chosen routes[12]. Thus, it is important that an attacker not be able to deflate the hop count of a route. This is what the hash chain mechanism seeks to prevent.

3.2 Analysis Using the New Model

In our analysis, we first define what correctness means for the hash chain mechanism in SAODV. Next, we choose the communication capabilities of the attacker we are modeling and discuss the implications of such capabilities. These implications are generally applicable. We then inspect hash chains under these implications and detail how this breaks the correctness for SAODV hash chains. Finally, we discuss the advantages that our top-down approach provides with respect to the security analysis.

3.2.1 Correctness

As stated in the previous section, the hash chain is meant to prevent nodes from falsely advertising short routes that do not exist in order to attract traffic. Therefore, if route discovery is started from a source S to a destination D, and node A is x hops away from S and y hops away[3] from D, then A should never be able to advertise a route from S to D with a hop count z such that $z < (x + y)$.

This is true for an ordinary node. Node A will receive a route reply (`RREP`) from D with the $Hash$ field set to $h^y(seed)$. Note that A will not know the seed value. Instead, it verifies the value of $Hash$ as per Equation 1. Since h is one-way, A cannot compute $h^i(seed)$ where $0 < i < y$. Therefore, its only opportunity to attack the route discovery process is to use the received Hop_Count and $Hash$ values for the forwarded message, failing to increment and rehash these values as per the SAODV protocol. Assuming that each of the remaining x hops proceeds to increment the Hop_Count field and rehash the $Hash$ field properly, then the resulting route reply advertises a route of verifiable length $(x+y)$ if A did not follow the protocol, or $(x+y+1)$ if A did follow the protocol. This is correct operation of the hash chain mechanism in securing the mutable Hop_Count field.

[3]Both hop counts are along the shortest route between the two nodes in question.

3.2.2 Implications of Attacker Communication Capabilities

For this analysis, we will be considering attackers with communication capabilities from Type III. As a reminder, Type III is characterized by a number of colluding devices, each of which has communication capabilities equivalent to that of a typical node in the network. However, together the devices have a larger sphere of influence.

Since the attackers are colluding, we assume that they share all knowledge gained during execution of the route discovery process. This sharing increases their computational capabilities since knowledge facilitates computation as depicted in Figure 3. In practice, the attackers will share this information either in-band (through routing messages tunnelled inside data packets) or out-of-band (through some other medium, e.g., wired, Bluetooth, GSM, CDMA). Regardless of how the attackers share this information, we can model the impact on the network as the union of a complete graph among the n attackers (K_n) with the existing graph representing the network topology.[4] A sample network is shown in the leftmost graph of Figure 4. In this graph, the attackers are denoted by solid black nodes. The complete graph among these attackers is shown in the center graph. The links in this graph represent their ability to pass information between them, whether in- or out-of-band. The rightmost graph is the union of the first two, representing the effect of the colluding attackers on the original network.

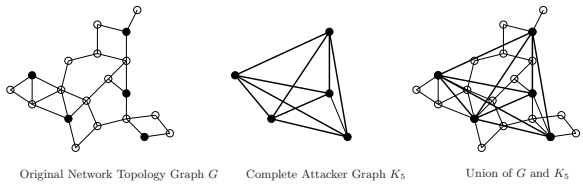

Figure 4: Impact of colluding Type III attackers.

3.2.3 Effect on SAODV Hash Chains

As previously stated, if route discovery is started from a source S to a destination D and node A is x hops away from S and y hops away from D, then A should never be able to advertise a route from S to D with a hop count z such that $z < (x + y)$. However, since we now have multiple attackers a slight adaptation of this correctness condition is required:

> Source node S is performing route discover to destination node D. Present in the network are n attackers $A_0, \ldots, A_{n-1}$. Attacker A_i is x_i hops from S and y_i hops from D. No attacker A_i should be capable of advertising a route shorter than $(x_i + y_i)$.

We will show that this correctness condition is easily broken by two attackers with Type III communication capabilities.

Consider a network in which two attackers A_0 and A_1 are present. Without loss of generality, we assume that A_0 is fewer hops away from S and A_1 is closer to D. When S is performing route discovery for D, A_0 will receive a routing message with $Hop\_Count = x_0$ and $Hash = h^{x_0}(seed)$. Using the direct communication channel from A_0 to A_1 (a result of the attackers having Type III capabilities), A_0 sends this routing message to A_1. A_1 can then broadcast this message towards the destination. When this message reaches D it will have

$$Hop\_Count = (x_0 + y_1)$$

and

$$Hash = h^{y_1}(h^{x_0}(seed)) = h^{x_0+y_1}(seed).$$

The hop count of this message will be successfully verified by D using Equation 1 and the attackers will thus have successfully advertised a route of length $(x_0 + y_1)$.

This breaks the correctness condition. As assumed earlier, A_0 is closer to S than A_1 which means that $x_0 < x_1$. Similarly, it was assumed that A_1 is closer to D than A_0 and thus $y_1 < y_0$. Therefore, $(x_0 + y_1) < (x_0 + y_0)$ and $(x_0 + y_1) < (x_1 + y_1)$. Thus, both attackers have advertised routes[5] shorter than any existing route from S to D passing through them.

3.2.4 Benefits of the Capabilities-Based Approach

Approaching the vulnerability in SAODV hash chains from the attackers' capabilities, it becomes clear that the ability to take messages from one area of the network and reuse them in another area is what breaks the security of SAODV's hash chains. From this conclusion we can determine that Type III communication capabilities are not the minimum necessary to perform this attack. In fact, Type II is the minimum required.

In addition, we have identified an important characteristic of attackers with Type II or higher communication capabilities. The ability to read messages in one area and write them to another not only exposes a flaw in hash chains, but also presents problems for any security mechanism that relies on ordered delivery or limited dissemination of messages. Also, it is important to note that since our model encourages the result to be stated in terms of the attackers' capabilities and properties of the security mechanism, future assessment of protocols for this vulnerability needs only to compare the protocol's requirements and the attacker under consideration to determine if it is vulnerable.

The ease with which this vulnerability was exposed demonstrates the benefits of the structured approach provided by our new model. Rather than relying on someone reviewing the protocol to recognize the existence of such a vulnerability by looking at the details closely, our model provides a framework for systematic analysis of protocols and the development of simple comparison-based tests for determining the vulnerability to previously analyzed attacks. The ability to distill the characteristics of the attacker and the root of the vulnerability for reuse in future analysis is a direct result of the capabilities-based approach.

4. CONCLUSION AND FUTURE WORK

In this paper we have presented a novel approach to modeling attackers for ad-hoc routing protocol analysis. Our new model looks at attacker capabilities rather than network topology and specific attack characteristics. In doing

[4]It should be noted, however, that since this may be in-band, it is not necessarily faster than data being routed over the existing network.

[5]A_1 advertises a "reverse" route of this length to D while A_0 advertises a "forward" route of this length to S

so, our model allows for better comparison of the security properties of existing routing protocols, as well as easier, more structured analysis of protocols developed in the future. Extensive future work remains to be done including further exploring the universal implications of specific attacker capabilities, categorizing known attacks based on the minimum attacker capabilities required, analysis of additional existing protocols, and expression of the security properties of these protocols in our model for comparative purposes.

5. REFERENCES

[1] G. Ács, L. Buttyán, and I. Vajda. Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 5(11):1533–1546, 2006.

[2] P. Argyroudis and D. O'Mahony. Secure Routing for Mobile Ad Hoc Networks. *IEEE Communications Surveys and Tutorials*, 7:2–21, 2005.

[3] C. N.-R. Baruch Awerbuch, David Holmer and H. Rubens. An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. In *ACM Workshop on Wireless Security (WiSe)*, Atlanta, Georgia, September 2002.

[4] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless Device Identification with Radiometric Signatures. In *MobiCom '08: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, pages 116–127. ACM, 2008.

[5] M. Burrows, M. Abadi, and R. Needham. A Logic of Authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990.

[6] L. Buttyán and I. Vajda. Towards Provable Security for Ad Hoc Routing Protocols. In *SASN '04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 94–105. ACM, 2004.

[7] C. Cremers and S. Mauw. chapter Operational Semantics of Security Protocols, pages 66–89. Lecture Notes in Computer Science. Springer, 2005.

[8] D. Dolev and A. Yao. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, Mar 1983.

[9] Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. *Ad Hoc Networks*, I:175–192, 2003.

[10] Y. Hu, A. Perrig, and D. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, 3:1976–1986, 2003.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne:: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In *MobiCom '02: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*, pages 12–23, New York, NY, USA, 2002. ACM Press.

[12] M. Jakobsson, S. Wetzel, and B. Yener. Stealth Attacks on Ad Hoc Wireless Networks. In *Proceedings of VTC, 2003*, 2003.

[13] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing*, volume 353. Kluwer Academic Publishers, 1996.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Mobile Computing and Networking*, pages 255–265, 2000.

[15] S. Nanz. *Specification and Security Analysis of Mobile Ad-Hoc Networks*. PhD thesis, Imperial College, London, 2006.

[16] P. Papadimitratos and Z. Haas. Secure Routing for Mobile Ad Hoc Networks. In *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002.

[17] 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*, pages 234–244, 1994.

[18] C. Perkins and E. Royer. Ad-Hoc On-Demand Distance Vector Routing. In *MILCOM '97 Panel on Ad Hoc Networks*, 1997.

[19] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. In *Cryptobytes, Volume 5, No. 2*, pages 2–13. RSA Laboratories, 2002.

[20] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. In *Mobile Computing and Networking*, pages 189–199, 2001.

[21] P. Ramachandran and A. Yasinsac. Limitations of On Demand Secure Routing Protocols. *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*, pages 52–59, 2004.

[22] M. G. Zapata and N. Asokan. Securing Ad Hoc Routing Protocols. In *WiSE '02: Proceedings of the ACM workshop on Wireless security*, pages 1–10, New York, NY, USA, 2002. ACM Press.