The Hierarchical Threat Model of Routing Security for wireless Ad hoc Networks

Guo Xian
College of Electrical and Information Engineering, Lanzhou University of Technology, GanSu LianHe University, LanZhou, China
iamxg@163.com

Feng Tao
School of Computer and Communication, Lanzhou University of Technology, LanZhou, China

Yuan Zhan-Ting
School of Computer and Communication, Lanzhou University of Technology, LanZhou, China

Ma Jian-Feng
School of Computer Science & Technology, Xidian University, Xi'an, China

Abstract: **The hierarchical threat model is proposed to address the issues that the *active-n-m* attacker model can't reflect the real capability of the attacker and the Dolev-Yao threat model is not fit for the security analysis of ad hoc routing. In hierarchical treat model, we appropriately extend the communication capability of the *active-n-m* attacker, and abandon the assumption that the adversary controls all of the communication paths in Dolev-Yao threat model. In addition, the number of nodes controlled by the adversary and the knowledge owned by the adversary are considered as the two important parameters to evaluate the attack strength. Lastly, we analyze the security of endairA and ARAN. Both of them are provably secure routing for ad hoc networks in *active-n-m* attacker model. But it has been proven that both of them have security flaws in the hierarchical threat model. The minimum attacker capability corrupted endairA and ARAN is identified in hierarchical threat model.**

Keywords: Ad hoc networks, routing security, the active-n-m attacker model, the hierarchical threat model, provable security.

1. Introduction

In wireless ad hoc networks, existing security routing protocols are evaluated in the traditional threat model, such as *active-n-m* attacker model [1]. It is assumed that the attacker has the same power and capability of a non-malicious node in the traditional threat model. This limitation which doesn't allow the attacker use out-of-band resources or other more powerful methods to corrupt a given routing protocol is not reasonable. In the traditional threat model, authors tend to claim protocol security based on a fixed environment. However, the security results are just only applicable if the protocol is analyzed under the author's assumptions of the attacker capabilities. These secure routing protocols may not be secure out of the respective assumptions [2-3]. Additionally, it is infeasible to compare multiple protocols without common assumptions or security definitions.

Because of its tractability, the Dolev-Yao attacker model [4] is the most prevalent model for security analysis of protocol such as authentication protocol. The Dolev-Yao attacker model can be disassembled into the following three assumptions: (1)Perfect cryptography, this assumption states that cipher-text can only be decrypted if the decryption key is present, and generated using encryption with the appropriate encryption key and plaintext. (2) Finite set of capabilities, an idealized attacker is defined which have a finite set of capabilities at his disposal. It is assumed that this attacker is equivalent to one which has an infinite set of capabilities which is playing according to the rules of perfect cryptography. (3) Omnipresence, the view that in order to prove a protocol correct, an attacker controlling all communication paths has to be considered. Following the first two assumptions is correct in ad hoc network. However, it is impossible to establish a view that an attacker in wireless ad hoc networks which would be "safe" in sense of the Dolev-Yao attacker, since the omnipresent attacker is imaginable but cannot be defended.

To address the above issues, new threat models are proposed in [5-6]. Inspired by these works, we develop the hierarchical threat model of routing security for ad hoc networks. Another contribution is to analysis security of two routings such as endairA [7] and ARAN [8] in our model. Both of them are provable security routing in extended *active-n-m* model [7, 9]. But we find they still have secure flaws in the hierarchical threat model.

2. The Hierarchical Threat Model

The hierarchical threat model analysis the attack strength of attacker for ad hoc routing from three aspects: the communication capability of the attacker, the number of nodes controlled by the adversary and the computation capability that mainly determined by the knowledge owned by the attacker. It is impossible or very costly, at least route layer, to defend against the Dolev-Yao attacker in ad hoc network environment, so we properly limited the communication capability of the attacker and don't intend to consider the Dolev-Yao attacker in our threat model. Advantages of our model are the followings: (1) in this model, we can analyze the security of a protocol runs in asynchronous and concurrent network environment. (2) Above all, developing a provable security routing protocol for ad hoc networks will be possible in this threat model. (3) Additionally, this model can also identify the minimum capability (beside of the Dolev-Yao attacker) required to break a routing protocol, and facilitate the security comparison of different protocols.

2.2 The Capability of Attacker

2.2.1 The Communication Capability

The attacker's communication capability can be down into *send* and *receive* capabilities. Reception of communication is a passive action in a wireless ad hoc network. Therefore, it is difficult to differentiate between a

978-0-7695-4207-2/10 $26.00 © 2010 IEEE
DOI 10.1109/ICNDC.2010.16

wireless device listening to messages within a typical transmission range and a device listening to messages from the entire network [6, 10]. Thus, we assume that if the attacker has the capability, it will choose to listen to the entire network in the hierarchical threat model. Sending messages is different from receiving in wireless ad hoc networks it is an active operation. There have been several proposals for identifying attackers who are transmitting messages to the entire network using a single identity, or using multiple identities with on a single radio transceiver. Therefore, such transmissions expose the attacker to an increased risk of detection [6, 10]. 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 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. So, in the hierarchical threat model, we give up the assumption that the attacker completely controls all of the communication paths. The communication capability of the attacker is properly limited and can be classified two following classes:

Type A: the communication capability of the attacker is the same as that of non-malicious node in the network. This class is denoted by T_A.

Type B: the reception capability of the attacker isn't limited and the sending capability of the attacker is the same as that of non-malicious node in the network. This class is denoted by T_B.

In fact, we can abstract out any special network topology configurations that may help enable an attack because of existing an unlimited reception attacker. 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.

Beside of the communication capability of the attacker, the attack strength of the attacker is largely relative to the number of nodes controlled by the attacker. By employing k node-disjoint routing paths between two communication nodes, the integrity and availability of the communication is guaranteed against DoS attackers of an attacker that controls less than k malicious nodes [11]. So, as the *active-n-m* attacker model, the number of nodes controlled by the adversary is considered as an important factor of the attack strength of the attacker in our model.

2.2.2 The Computation Capability

The computation capability of the attacker is also closely relative to the attack strength of the attacker. The computation capability of the attacker is mainly determined by the knowledge owned by the attacker. For instance, the attacker can easily decrypt the cipher-text, if it has the valid key. In modern network environment, the attacker can also use information captured from different session instances of different protocols or same protocol to compromise a protocol. Therefore, beside of considering the feasibility that the attacker compromise cryptographic scheme, it is necessary to determine what information can be available to the attacker that corrupt an ad hoc routing protocol.

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 an insider node in a network, there is some initial knowledge that it will have which includes key material and other parameters. Additionally, Collusion among several attackers not only increases the information available as colluding attackers, but it also increases the information available as colluding attackers share all key material, nonce, hash chain seeds, etc. in order to be more powerful.

Therefore, the knowledge such as the initial knowledge possessed by the attacker and especial information that can be captured by the attacker during execution of a protocol is considered to evaluate the attack strength of the attacker in the hierarchical threat model. Our model has the capability that analyzes the possibility that the attacker performs *concurrent attack* [12]. The concurrent attack is an attack against an ad hoc routing protocol. It is implemented by using the information that captured from different session instances of a protocol or different protocols run in asynchronous and concurrent network environment. An attack that shown in this paper against a provable security ad hoc routing endairA [7] is the concurrent attack completed by using the information captured from different session instances of a protocol and constructing the valid signature of some non-malicious nodes.

2.2.3 Formal Description of the Hierarchical Threat Model

To summarize, the attack strength of the adversary in the hierarchical threat model is determined by the following three parameters:

(1)n, the number of nodes that the attacker owns.

(2)the communication capability of the attacker, denoted by the symbol *ccap*. The value of *ccap* is T_A or T_B.

(3)S_{inf}, the attacker's initial knowledge and the information captured during network operation.

Thus, we formalize the attacker as *attacker*(n, *ccap*, S_{inf}). The communication capability of the attacker is appropriately limited. The model not only takes into account the case of a single attacker (n=1), but also that of multiple attacker collusion (n>1). The attack strength is closely relative to the knowledge owned by the attacker. To reason about the information that the attacker can derive if it posses certain knowledge, we can use any of several methodologies such as the axioms in PCL [13]. We offer the attack classification shown in table 2.1.

Apparently, *attacker*($1,T_A,\{key\}$) in our model is equal to *active-1-1* attacker. And *attacker*(m, T_A, $\{key_1, key_2, \ldots, key_n\}$) is identical to *active-n-m* attacker ($m \geq n$). That is to say, a protocol can effectively defend against *active-n-m* attack if it can defend against A_5 attack in the hierarchical

Table 2.1 The Attacker Classification

The node number *n* owned by the attacker	The communication capability	The computation capability		Insider/ Outsider	The attacker category	Attacker Goal
		The knowledge	The key			
n=1	T_A	Initial knowledge	No	Outsider	A_1	Corrupt Route /Add self to route
			Yes	Insider	A_2	Corrupt Route
	T_B	Initial knowledge and information captured from network	No	Outsider	A_3	Corrupt Route /Add self to route
			Yes	Insider	A_4	Corrupt Route
n>1(Collusion)	T_A	Initial knowledge	Yes	Insider	A_5	Corrupt Route
	T_A	Share initial knowledge and information captured form network	Yes	Insider	A_6	Corrupt Route
	T_B	Share initial knowledge and information captured form network	Yes	Insider	A_7	Corrupt Route

threat model. And we can easily draw the following propositions.

Proposition 1: a protocol can effectively defend against A_1 attack, if it is secure in presence of A_2 attacker in table 2.1.

Proposition 2: a protocol can effectively defend against A_1, A_2, A_3 attack, if it is secure in presence of A_4 attacker in table 2.1.

Proposition 3: a protocol can effectively defend against A_1, A_2, A_3, A_4, A_5 attack, if it is secure in presence of A_6 attacker in table 2.1.

Proposition 4: a protocol can effectively defend against A_1, A_2, A_3, A_4, A_5, A_6 attack, if it is secure in presence of A_7 attacker in table 2.1.

The proof of the above propositions is omitted.

3. Application of the Hierarchical Threat Model

On-demand routing for Ad hoc networks can be classified two main classifications: On-demand source routing, such as DSR[14] etc, On-demand distance vector routing such as AODV[15] etc. Some secure routings based on DSR and AODV, such as endairA, SAODV [16], ARAN etc, are developed by introducing cryptographic schemes. But secure flaws in them are sequentially found.

3.1. endairA and Security Analysis of endairA

3.1.1. Overview of endairA

Inspired by Ariadne, the authors designed a routing protocol and called it endairA in [7]. The protocol is based on DSR and is a provable security routing protocol in ABV model. The route discovery process is shown in Fig. 3.1.

*S->**: (*rreq, S, T, id,* ())
*A->**: (*rreq, S, T, id,* (*A*))
*B->**: (*rreq, S, T, id,* (*A, B*))
T->B: (*rrep, S, T, id,* (*A, B*), (sig_T))
B->A: (*rrep, S, T, id,* (*A, B*), (sig_T, sig_B))
A->S: (*rrep, S, T, id,* (*A, B*), (sig_T, sig_B, sig_A))

Fig. 3.1. The Route Discovery Process of endairA

3.1.2. Security Analysis of endairA

It has been proven that endairA is a provable security routing for Ad hoc network in ABV model. However, it has been proven that two colluding attackers can initiate a concurrent attack by capturing information from different session instances of same protocol or different protocols and further constructing the signature of some non-malicious participants.

Theorem 1: endairA can't defend against *attacker*(2, T_A, {key_1,key_2,…}) in the hierarchical threat model. That is, endairA is not secure in presence of A_6 attack in the hierarchical threat model. In *attacker*(2, T_A, {key_1,key_2,…}), key_1 and key_2 are compromised key that the attackers can share and '…' stands for the information that the attackers may capture from network during execution of a protocol.

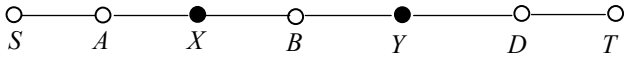

Fig. 3.2. An Attack Scenario for endairA

Proof: The proof is similar to that of [12]. Consider an instance of endairA with source node *S* and let (*S*, *A*, *X*, *B*, *Y*, *D*, *T*) be a sequence of identifiers of pairwise neighbor nodes in Fig. 3.2, in which on *X* and *Y* are compromised nodes. In the attack, when the second node *Y* receives

RREQ=(*rreq, S, T, id*$_1$, *routelist*= (*A, X, B*))

it drops node *B* from the listing and transmits:

RREQ=(*rreq, S, T, id*$_1$, *routelist*= (*A, X, Y*))

Eventually, the route request will reach the target *T* that

will compute and send back a route reply. Node Y will receive from D:

$$RREP=(rrep, S, T, id_1, routelist=(A, X, Y, D), sig_T, sig_D) \quad (3.1)$$

Now, Y can obviously attach its identifier and signature to this reply and transmit to B the extended reply, but B will not re-transmit it because B is not included in the listing. So Y initiates a new route discovery session with source Y and target X, and sends to B a route request:

$$RREQ=(rreq, Y, X, id_2)$$

with an identifier id_2 that contain the information required to construct the signatures sig_T, sig_D in message (3.1), the identifier D, and the signature sig_Y of Y (if this is needed). The identifier id_2 will most likely not be long enough for this purpose, so node Y has to initiate several route discovery process using identifiers id_3, id_4, etc, to get all the bits required. Eventually, X will be able to reconstruct the signatures, and generate the route reply:

$$RREP=(rrep, S, T, id_1, routelist=(A, X, Y, D), sig_T, sig_D, sig_Y, sig_X)$$

which is send back to the source S and validated.

Clearly, the instances with the identifiers id_1, id_2, … , are different instances of protocol sessions. The attacker can make use of information such as the signatures sig_T, sig_D of non-compromised nodes, which are constructed according to the knowledge captured from instances with identifiers id_2, id_3, etc, to corrupt the route discovery process with identifier id_1 and result in an incorrect route (a route that is not consistent with the current network topology) which is accepted by the source. Namely, endairA can't defend against *attacker*(2, T_A, {key_1, key_2, … }), where '…' indicates the knowledge owned by the attacker.□

Theorem 2: if the compromised nodes are not neighboring, endairA can defend against *attacker*(m, T_A, {key_1, key_2, … , key_n})($n \le m$). That is, endairA is secure in presence of A_5 attack in the hierarchical threat model. In *attacker*(m, T_A, {key_1, key_2, …, key_n}), key_1, key_2,…, key_n are compromised keys that the attackers can only share.

We have known that the capability of *attacker*(m, T_A, {key_1,key_2, …, key_n}) in the hierarchical threat model is equal to the capability of *active-n-m* attacker ($m \ge n$). The proof of *Theorem* 2 is similar to [7]. However, if the adversary controls several neighboring compromised nodes, the adversary can control all of communication paths in sub-network formed by these neighboring and compromised nodes. In term of this sub-network, the capability of this attacker is identical to that of the Dolev-Yao attacker. So, it is difficult or impossible to develop a provable security routing that can defend against this attack. To avoid the analysis for this attack, neighboring compromised nodes that they can share information are merged into a single node in the ABV threat model [7, 9], but which result in incorrect routes are accepted by the initiator of the route discovery process.

The hierarchical threat model gives up the attempts analyzing security of routing in presence of Dolev-Yao attacker, such that we can develop a provable security routing in this model. So, the minimum capability corrupting endairA in the hierarchical threat model is that the attacker can compromised more two nodes and these compromised nodes can share information captured from network. endairA can't defend against A_6 attack in our model.

3.2. ARAN and Security Analysis of ARAN

3.2.2. Overview of ARAN

Source Identity
Source Sequence Number
Last Hop Identity
Next Hop Identity
Hop Count
Expiration Timer

Fig. 3.3. The Routing Table of AODV

ARAN based on AODV is a secure routing protocol for ad hoc networks. The routing messages do not contain information about the whole route path, but only about the source and the destination. The route table of some node records the path that gets to the destination through the node. The routing table is shown in Fig. 3.3. ARAN uses public key cryptography to ensure the integrity of routing messages. The route discovery process that establishing a route such as (*S, A, B, T*) is shown in Fig. 3.4. Where, S and T are the source and the target of the route discovery, respectively. l_i is the identifier of node i, sig_{l_i} is the signature of node of the identifier l_i on all of these elements and $cert_i$ is the public-key certificate of node i. N_i is a nonce generated by i, t is the current time-stamp. RREQ and RREP respectively indicate that this message is the route request and the route reply.

$$S->*: sig_{l_S}(RREQ, l_T, cert_S, N_s, t), cert_S$$
$$A->*: sig_{l_A}(sig_{l_S}(RREQ, l_T, cert_S, N_s, t)), cert_A$$
$$B->*: sig_{l_B}(sig_{l_S}(RREQ, l_T, cert_S, N_s, t)), cert_B$$
$$T->B: sig_{l_T}(RREP, l_S, cert_T, N_s, t), cert_T$$
$$B->A: sig_{l_B}(sig_{l_T}(RREP, l_T, cert_T, N_s, t)), cert_B$$
$$A->S: sig_{l_A}(sig_{l_T}(RREP, l_T, cert_T, N_s, t)), cert_A$$

Fig. 3.4. The Route Discovery Process of ARAN

3.2.2 Security Analysis of ARAN

It has been proven that ARAN is a secure routing for Ad hoc networks in ABV model [7]. In this paper, we state that ARAN is indeed secure against a single attacker or multiple non-colluding attackers whose transmission is limited. But we prove that ARAN cannot defend against the colluding attack performed by the attackers with non-limitation reception in hierarchical threat model.

Theorem 3: The probability that ARAN is compromised by the adversary *attacker*(1, T_B, {*key*}) (*key* is initial key of a malicious node.) is negligible, if the signature scheme

used in ARAN is secure against chosen message attacks in hierarchical threat model.

This proof of this theorem is similar to that of [9].

In fact, ARAN is also secure against *attacker*(n, T_A, {key_1,…, key_n}), since the threat of multiple attackers that the communication capability is the same as non-malicious node in the network is identical to that of an single attacker. But the following theorem shows that ARAN cannot defend against *attacker*(2, T_B, {key_1, key_2}).

Theorem 4: ARAN can't defend against *attacker*(2, T_B, {key_1,key_2}) (key_1,key_2 are valid keys that two malicious insider can share).

Proof: We assume that the source S and the destination T are honest, and that v and v' are two compromised nodes controlled by the attacker and are the nodes in transmission range of the source S. key_1 and key_2 are respectively initial keys of v and v'. Let us further suppose that S initiates a route discovery process and the attacker later receives a route reply message RREP from one neighbor of v on the malicious node v. On the malicious node v, the attacker *attacker*(2, T_B, {key_1, key_2}) can sign the RREP in the name of v' and then can unicast the RREP to the source S, since the reception capability of *attacker*(2, T_B, {key_1, key_2}) isn't limited and the attacker can share initial keys key_1 and key_2.

When the RREP with the signature of the malicious node v' reaches the compromised node v, this signature for the RREP can be verified. So, the comprised node v' is considered as the next hop node, but there is no a route entry from the comprised node v' to the target in routing table of the node v'. Thus, the adversary *attacker*(2, T_B, {key_1, key_2}) successfully corrupts ARAN, that is, ARAN cannot defend against *attacker*(2, T_B, {key_1, key_2}).

4. Conclusion and Future Work

In our model, we appropriately limit the communication capability of the attacker, and introduce two important parameters such as the number of nodes controlled by the adversary and the knowledge owned by the adversary to evaluate the attack strength. In contrast to the old two models, the hierarchical threat model can analyze the security of routing protocol which runs in asynchronous and concurrent network environment and make it possible to develop a provable security routing for ad hoc network. Of course, the hierarchical threat model can also identify the minimum attacker capability which breaks a given protocol and can facilitate the security comparison between different protocols. Extensive future work remains to be done including further exploring integration of our threat model and formal analysis technique of secure routing protocol, analysis of additional existing protocols, and expression of the security properties of these protocols in our model for security analysis purpose. Especially, it is the future main work that developing provable security routing protocol for Ad hoc networks in our treat model.

5. References

[1] Y. C. Hu and A. Perrig. "A survey of secure wireless ad hoc routing". IEEE Security & Privacy, vol. 2(3), 2004, pp: 28-39.

[2] D. Djenouri, L. Khelladi, and A. N. Badache. "A survey of security issues in mobile ad hoc and sensor networks", IEEE Communications Surveys & Tutorials, vol. 7(4), 2005, pp. 2-28.

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

[4] D. Dolev and A. Yao."On the security of public key protocols". IEEE Transactions on Information Theory, vol. 29(2), 1983, pp. 198-208.

[5] Todd R. Andel, Alec Yasinsac. "Adaptive threat modeling for secure ad hoc routing protocols". Electronic Notes in Theoretical Computer Science (ENTCS). vol. 197(2), 2008, pp. 3-14.

[6] Jared Cordasco, Susanne Wetzel. "An attacker model for MANET routing security". In proceeding of the second ACM conference on wireless network security. Zurich, Switzerland, 2009, pp. 87-94.

[7] Gergely Acs, Levente Buttyan, and Istvan Vajda. "Provably secure on-demand source routing in mobile ad hoc networks". IEEE Transactions on Mobile Computing, vol. 5(11), 2006, pp. 1533-1546.

[8] Sanzgiri, K.Laflamme, D. Dahill, B. Levine, B.N. Shields, C. Belding-Royer, E.M. "Authenticated routing for ad hoc networks", Selected Areas in Communications, vol. 23(3), 2005, pp. 598-610.

[9] Gergely Acs, Levente Buttyan, and Istvan Vajda. "Provable security of on-demand distance vector routing in wireless ad hoc networks". In proceeding of 2th European workshop on Security and privacy in Ad hoc and Sensor Networks (ESAS 2005), Springer press, LNCS 3813, 2005, pp. 113-127

[10] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. "Wireless Device Identification with Radiometric Signatures". In proceeding of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom'08), 2008, pp. 116-127.

[11] Panayiotis Kotzanikolaou,Rosa Mavropodi,Christos Douligeris. "Secure Multi-path Routing for Mobile Ad hoc Networks", Ad hoc networks, vol. 5(1), 2007, pp. 87-99.

[12] Mike Burmester and Breno de Medeiros . "On the Security of Route Discovery in MANETs". IEEE Transactions on Mobile Computing, vol. 8(9), 2009, pp. 1180-1188.

[13] Anupam Datta, Ante Derek, John C. Mitchell. "Protocol composition logic (PCL)", Electronic Notes in Theoretical Computer Science, vol. 172(1), 2007, pp. 311-358.

[14] David B. Johnson and David A. Maltz."Dynamic Source Routing in Ad Hoc Wireless Networks". Mobile Computing, vol. 12(6), 1996, pp. 10-23.

[15] C. Perkins and E. Royer."Ad hoc on-demand distance vector routing". Mobile Systems and Applications. vol. 24(3), 1999, pp. 59-81.

[16] M. Guerrero Zapata and N. Asokan. "Securing Ad Hoc Routing Protocols". In Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.