Advances in Computer Science Research (ACSR), volume 61
7th International Conference on Education, Management, Computer and Society (EMCS 2017)

Security Analysis and Application of Common Dynamic Routing Protocol

Shoubai Xiao

Nanchang Institute of Science & Technology, Jiangxi Nanchang 330108

Keywords: Mobile Ad Hoc network; Dynamic routing; Security threats

Abstract. Mobile Ad Hoc network is a kind of multi-hop wireless network without infrastructure. The network node is both a host and a router. The secure routing protocol can obtain trusted path information only by relying on all the trusted nodes in the network, which needs to use cryptographic security protocol to achieve. However, the analysis of routing protocol security is different with the security of analysis of cryptographic security protocol, and the behavior of network intermediate nodes that composing the network must be considered. Therefore, the formal analysis technology for cryptographic security protocol cannot be directly used for the security analysis of secure routing protocols. The new method of designing and analyzing secure routing protocols has important theoretical and application value.

Introduction

Dynamic routing is the process of updating the routing table by exchanging routing information between routers in the network. It can flexibly adapt to the dynamic changes of the network topology and automatically update the routing information, which is suitable for larger and more complex network topology, but it will take up network bandwidth and CPU resources to varying degree. In practical applications, dynamic routing is usually taken as the complementation of static routing. When a packet is routing in the router, static route is looked up firstly. If it exists, forward packet based on static routing, unless find dynamic routing. According to the operation mode of the protocol, dynamic routing protocol can be further divided into distance vector routing protocol, link state routing protocol and hybrid routing protocol. In addition, routing protocols can be divided into classified and unclassified routing protocols. The classified routing protocols exchange route updates between routers without subnet mask; unclassified routing protocols are just the opposite.

This paper analyzes the existing routing security model active-n-m, attack model, parametric threat model and adaptive threat model. Based on the Dolev-Yao attack model and the characteristics of existing threat model, this paper proposes a hierarchical threat model that is more suitable for modeling routing security threats.

Analysis of Common Dynamic Routing Protocol

The common dynamic routing protocols usually include:

Folding RIP

Routing Information Protocol (RIP) is the first widely used protocol in the internal gateway protocol IGP. It is a distributed routing protocol based on distance vector. It is the standard protocol of Internet. Its biggest advantage is simple and costly.

Folding OSPF

OSPF (Open Shortest Path First) is an internal gateway protocol (IGP) for routing decisions within a single autonomous system (AS).

Folding IS-IS

IS-IS (Intermediate System-to-Intermediate System) is a kind of dynamic protocol designed by ISO (the International Organization for Standardization) for CLNP (Connection Less Network Protocol).

Folding BGP

Border Gateway Protocol (BGP) is a routing protocol for an autonomous system running on TCP. BGP is the only protocol used to handle networks like Internet-size and is the only multi-drop connection protocol that can handle properly unrelated routing domains.

Routing Security Threat Model

Active-n-m Threat Model. In the routing protocol design and security analysis of Ad hoc Network (MAN Ads), the active-n-m threat model is a widely used traditional threat model. N in the active-n-m threat model is the number of attacked nodes with the authentication key, and m is the number of network nodes controlled by the attacker. Any attacked node in the active-n-m threat model has the ability to distribute attack key to other m-1 nodes. However, the main problem with this model is that all the attacked nodes and network nodes controlled by attackers have the same communication capability, and the attacker's attack ability is related to the actual network topology, and does not allow the attacker to control the shared node Information that is captured during runtime.

It's the threat model combined active-n-m threat model and abstract network model. The undirected graph G (V, E) referring to wireless network topology in this model is defined as a network structure conf (configrations). In the network structure, the adjacent attack nodes are merged into a single node, as shown in Fig. 1, where nodes A1, A2 and A3 represent the attack nodes controlled by the attacker, and the merged single attack nodes, such as A1, 2 and A3, are limited in the transmission capacity of a single node in transmission capacity, Their communication capabilities are the same with common nodes, limiting the ability of attackers.

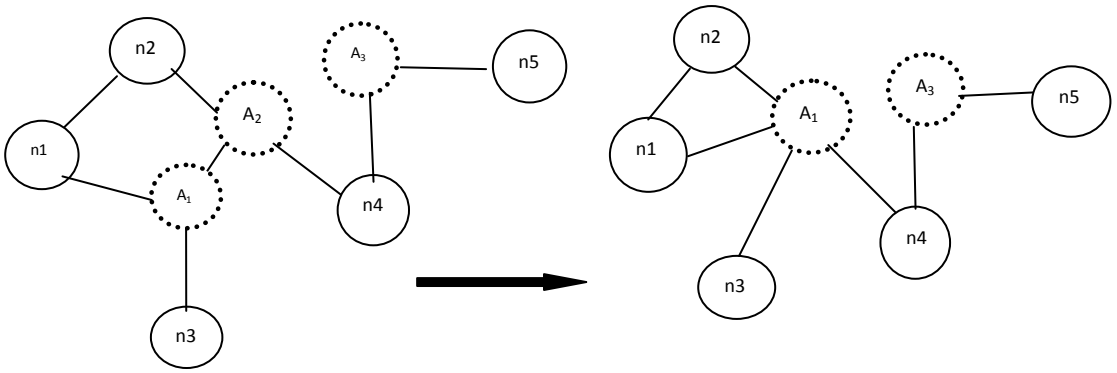

Figure 1. Network structure conf

Dolev-Yao Threat Model. The Dolev-Yao threat model is a formal threat model for the cryptographic security protocol. The attacker in the Dolev-Yao threat model is characterized by: (1) the attacker can monitor all the messages on the communication link; (2) the attacker is trusted user and can initiate a communication connection to any node; (3) an attacker can act as a connection target for any node. The Dolev-Yao threat model typically models the source nodes that communicate with each other and the target nodes into communication end nodes, modeling the attacker into a controller of the communication link or a central entity that forwards all communication data, as shown in Fig 2. As the end-to-end security requirements do not have to take the behavior of intermediate nodes on the communication path into account, which can effectively encapsulate attacks against security requirements of security protocols to simplify the analysis.

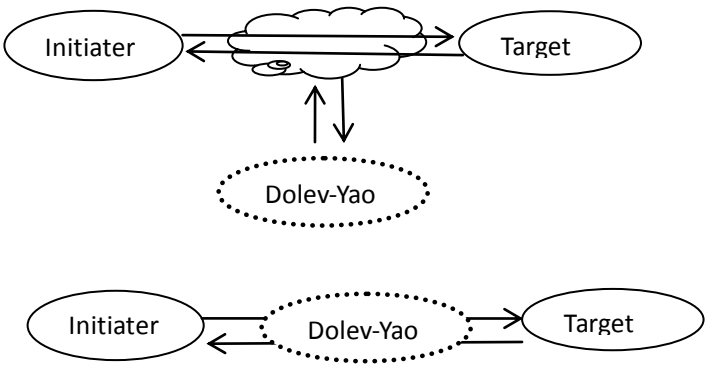

Figure 2. Dolev-yao threat model

The threat of the attacker to router security in the Dolev-Yao threat model can be shown in Fig 3. Node A in Figure 3. represents the node controlled by the attacker. An attacker can capture any message in the network and be able to deliver messages to any network node. And because the communication between any two nodes can be effectively simplified as the two-hop network communication existing communication channel between the attacker and two nodes. The attacker can easily shorten the route to achieve the attack on the routing protocol, or the attacker having Dolev-Yao threaten model's ability can attack the entire network by deleting the received message, thus destroying the target of the communication path established by the routing protocol to establish.

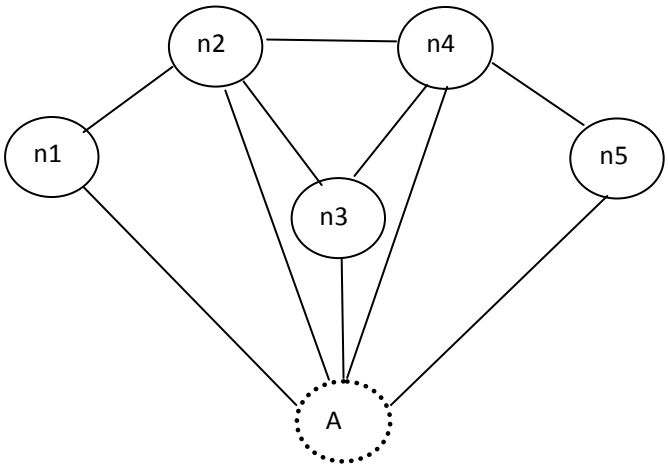

Figure 3. Threatening of Dolev-Yao attackers for routing security

Therefore, although the Dolev-Yao threat model can provide the strongest formal threat model, the Dolev-Yao threat model cannot be directly used to evaluate the security of Ad hoc network routing protocols. The secure routing protocol must ensure that the routing discovery process return can reflect the communication path of current network topology information to ensure the integrity and reliability of it and relying on the intermediate node on the communication path to transfer data between the source node and the target node. Therefore, when evaluating a secure routing protocol, the behavior of intermediate node cannot be ignored. The threat model must take the behavior of

intermediate node into account. In addition, a reasonable routing security threat model must prevent protocol designers from preventing attacks that cannot be eliminated at the routing layer or at a significant cost to eliminate them.

Security Analysis of Dynamic Routing

Security of RIP Protocol. As an earlier version, RIP protocol has relatively large security vulnerabilities, due to the continuous upgrading and development of the network. In the current network structure, RIP protocol is often used by associating with other routing protocols. Thus the other routing protocols often reassign the updated information submitted by RIP. If the attacker spoofs the network with the RIP protocol, it can cause the attack scope to be expanded if it is allocated again through other types of protocols that are not authenticated. In the earlier case that the network is relatively simple, RIP can be a very good network. But with the continuous development and its own insecurity factors to be exposed, because there is no use of authentication mechanism, and the use of low reliability UDP protocol transmission, deception is relatively easy. In the modern case, o use RIP protocol, 16-character civilized password or MDK signature is offer set in the protocol options. In this case, the difficulty to make attacker's deceitful information will be greatly improved, so as to improve the security of the protocol.

Security of OSPF Protocol. OSPF security performance has been greatly improved. It uses a verification mechanism; only the information through the verification and getting trust can spread between the routers. The authentication mechanism is generally classified as null authentication, simple password authentication and encryption authentication. To find loopholes when improving the security, due to the use of authentication mechanism and chain information diffusion, the attacker is often easier to intercept civil information through producing camouflaged routing information and analysis of network model, so for the network communication resources occupation, the router resource has been in a busy state, and there is a significant reduction in the proportion of information transmission. It's easy to forge the null authentication and simple password verification for the attackers and encryption verification in the higher-level technology for encryption and tampering and replay of attack vulnerabilities often adopt more reasonable password technology to solve, for example, using asymmetric encryption technology, that is, digital signature. The information in the digital signature contains the number of routers in network, the way of area division, and refresh rate to a series of information. The difficulty for attackers to forge is greatly improved.

Conclusion

With the rapid development of computer network technology and continuous expansion of network planning, network structure will continue to be complicated, so in the development of computer network routing, communication routing protocol security analysis should be paid special attention. As the core and fundamental of network transmission, routing protocol is directly related to the transmission speed and security of network data. Therefore, when the attack mode and vulnerability exploration are diversified, the routing protocol security measures should be improved without being attacked. To avoid harming the network, this paper illustrates various routing protocols, which has a good guiding significance for building a network system.

★ Project Supported by: Nanchang Key Laboratory of Intelligent Building Network Engineering

References

[1] Filaretov V, Gorshkov K, Mikheenko A. A circuit synthesis technique based on network determinant expansion[C]// International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications To Circuit Design. IEEE, 2012:293-296.

[2] Horie T, Hasegawa G, Murata M. Proactive recovery method against multiple network failures with overlay networking technique[C]// Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International. IEEE, 2010:1-6.

[3] Liu T. A Review of Network-based Storage Technique[J]. Computer & Digital Engineering, 2011.

[4] Pattaranantakul M, Janthong A, Sanguannam K, et al. Secure and efficient key management technique in quantum cryptography network[C]// Fourth International Conference on Ubiquitous and Future Networks. IEEE, 2012:280-285.

[5] Lee S H, Jo A R and Choi G P, et al. Fabrication of 3D alginate scaffold with interconnected pores using wire-network molding technique[J]. Tissue Engineering and Regenerative Medicine, 2013, 10(2):53-59.

[6] M She, H Yang and J Tang, Research on the practical teaching system for Computer Network Technique based on skill competitions and its applications[C]// International Education, Economics, Social Science, Arts, Sports and Management Engineering Conference. 2016.

[7] Mastan J M K, Sathishkumar G A, Bagan K B. A Color Image Encryption Technique Based on a Substitution-Permutation Network[C]// International Conference. DBLP, 2011:524-533.

[8] Y.Q Zhang, The Application of Network Technique in the University Administrative Management[J]. Computer Knowledge & Technology, 2010.

[9] Hirnwal S, Chauhan K and Gupta A. Intrusion Detection Technique in Mobile Adhoc Network Based on Quantitative Approach[J]. International Journal of Computer Applications, 2012, 37(8):22-27.

[10] Sikiru T H, Jimoh A A, Agee J T. Optimal location of network devices using a novel inherent network topology based technique[J]. 2011:1-4.

[11] Ali D, Abdullahi M, Application of Wavelet De-noising Technique on a Congested Internet Protocol (IP) Network[J]. International Journal of Computer Applications, 2014, 100(5):12-15.

[12] F.L Wang, Discovery and Analysis about Computer Network Security Technique and Prevention Strategy[J]. Computer Security, 2010.