Black Hole Attack Injection in Ad hoc Networks

Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil
Fault Tolerance Systems Group (GSTF), Instituto de las TIC Avanzadas (ITACA)
Universidad Politécnica de Valencia, Campus de Vera s/n, E-46022, Valencia, Spain
{ jcruizg, jefrilo, ddandres, pgil}@disca.upv.es

Abstract

Ad hoc networks exploit the processing, storage and wireless communication capabilities of mobile devices to create spontaneous and low-cost self-configuring networks. Despite the promises offered by such networks, their industrial exploitation claims for methodologies to assess the level of security provided by resulting solutions. A first step towards that ambitious goal is to study how central elements of ad hoc networks, their routing protocols, behave in absence, but also in presence, of malicious faults (attacks). Black holes are simple but effective denial of service attacks in today's ad hoc networks. This paper describes how to inject such attacks in ad hoc networks relying on proactive routing protocols. A VoIP ad hoc solution is used as case study.

1. Introduction

In ad hoc networks, devices rely on each other to keep the network connected. Thus, unlike traditional wireless solutions, such networks do not require any pre-existent (fixed) infrastructure, which minimize their cost and deployment time. Ad hoc networks are gaining momentum in many different application domains, like emergency, military-tactical and civilian environments.

Routing protocols enable multi-hop communications in ad hoc networks. To achieve availability, routing protocols should be robust against both topology changes and malicious attacks. Existing protocol specifications cope well with the change of network topologies. However, defence against malicious attacks has remained optional. Nowadays, the trend is changing and there is an increasing interest on research focused on the provision of proposals for securing ad hoc routing protocols [1]. This research claims for methodological approaches to (i) evaluate the robustness of routing protocols against attacks and (ii) assess the effectiveness of security enhancements.

This paper copes with this lack and takes a step forward to the provision of tools for auditing the security of ad hoc routing protocols. Due to space limitations, reported research is limited to the description of how black hole attacks can be injected in proactive routing protocol-based ad hoc networks. Section 2 describes the threats of such networks. Section 3 specifies the attack injection approach, whose feasibility is illustrated in Section 4. Section 5 concludes this paper.

2. Ad hoc network threats

In ad hoc networks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it [1].

There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures.

The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today.

3. Attack approach

The attack approach proposed in this paper copes with the aforementioned challenge. It structures in two successive steps (see Figure 1):

1. *The malicious node (M) induces a network topology propitious for the attack success (Figure 1.b).* To cope with that goal (i) M induces a possible routing link between attack targeted devices (call them A and D), then (ii) M emits protocol-compliant messages for leading both A and D to choose such link for their communications.

2. *M carries out the attack (Figure 1.c).* In the case of a black hole attack, M drops (does not retransmit) the packets. This packet dropping can be selective (it only affects a particular type of packets) or not (all packets are black holed).

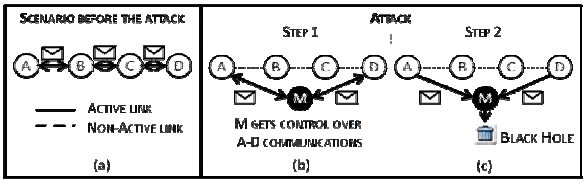

Fig. 1: Attack approach

The detailed description of other type of attacks is out of the scope of this paper. However, it must be mentioned that M can carry out other type of attacks by simply changing the way it manipulates the intercepted packets (see Figure 1.c). For instance, it can forge new packets or modify, delay or reorder intercepted ones.

Once the attack has been injected, its impact in the network communication and the running applications must be evaluated. This impact may, for instance, lead a particular application to fail, degrade network communications, isolate nodes or create routing loops.

4. Case study

The considered ad hoc network was executed using the CASTADIVA test-bed [2]. The network integrates four nodes, named A, B, C, D, and initially has the topology shown in Figure 1.a. Nodes A and D are Ubuntu-based laptops communicating using a VoIP application (called Ekiga [3]). Thus, an Ekiga client runs on each of these laptops. The other intermediate nodes (B and C) act as routers and are executed inside OpenWRT-based Linksys access points [4]. The ad hoc network relies on the use of a proactive routing protocol, named OLSR [5]. It employs periodic exchange of messages to maintain updated network topology (routing) information at each node. The version of the protocol executed in all the considered network nodes is the v0.4.10.

The goal of the malicious node M (a B-/C-like node) consists in black holing all VoIP-related packets exchanged by A and D. If the attack meets its objective, then video and sound flows between A and D will be dropped, thus terminating the VoIP call.

Initially M is not part of the network. Among all possible topologies suitable for the attack, M induces the one showed in Figure 1.b by faking HELLO and TC OLSR messages. According to the protocol specification, HELLO messages are used for link sensing, neighbour detection and multipoint relay (MPR) signalling. The set of MPRs of a node is defined by the set of its neighbours that "cover" all 2-hops neighbourhood. MPRs are used by nodes to perform topology declaration by transmitting Topology Control (TC) messages. Such messages enable nodes to determine optimal routes for their communications.

M forces the topology shown in Figure 1.b by (maliciously) misusing the aforementioned messages. It starts injecting in the network HELLO messages declaring A and D as neighbours, and TC messages to announce the links with them, i.e. (M→A and M→D). To obtain a symmetric link, M needs A and D to generate TC messages announcing links A→M and D→M. To avoid the generation of these messages at the victims (A and D) side, M forges fake TC messages announcing such links. It sets the victim's address in the originator field of the TC message. It must be noted that this attack step is transparent to A and D, since it does not affect the VoIP call.

Once the link created, M drops all the VoIP traffic related to the A and D conversation. This is done by instructing M's internal firewall (ip tables) with the adequate filtering rules. As a result, the conversation between A and D cannot progress. In our case, the attack leads Ekiga clients running in A and D laptops to freeze video and stop reproducing voice. Such anomalous behaviour shows a vulnerability of the evaluated protocol against the injected attack.

5. Conclusion

This paper shows practically how to perpetrate black hole attacks in ad hoc networks. This research defines a first effort towards the definition of an attack injection framework for auditing the resilience of ad hoc routing protocols and discovering new vulnerabilities in such communication elements.

6. Acknowledgements

This work has been partially sponsored by the Spanish TecnoSeC project (MEC TIN2006-08234), the European EUREKA-CELTIC RED project (CP3-011).

7. References

[1] Hao Yang et al., "Security in mobile ad hoc networks: challenges and solutions**"**, IEEE Wireless Communications, Volume 11, Issue 1, Page(s): 38 – 47, Feb. 2004.

[2] J. Hortelano et al., "Castadiva: A Test-Bed Architecture for Mobile AD HOC Networks", 18th IEEE Int. Symp. PIMRC, Greece, Sept. 2007.

[3] Ekiga [Online] Available: http://ekiga.org.

[4] OpenWrt [Online] Available: http://openwrt.org.

[5] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, Oct. 2003.