

WSN Security: Wormhole Attack

Ahmed LOUAZANI
Computer science department,
Hassiba Benbouali University, Chlef
alouazani@gmail.com

Abstract (Computer and WSN security)

The term computer security which is frequently used means saving each of hardware, user and system programs and data from any possible attack. The risk of attacks increases when connecting computer to network, especially the Internet. The major technical areas of computer security are usually represented by the initials CIA: confidentiality, integrity, and authentication or availability.[JF.K 07] (see Figure1).

The nature of wireless ad hoc and sensor networks (Due to the special characteristics of WSNs, e.g. low processing and energy resources and ad hoc networking [Pan 06]) make them very attractive to attackers. One of the most popular and serious attacks in wireless ad hoc networks is wormhole attack. Here the adversary connects two distant points in the network using a direct low-latency link which can be established by various means (wired link, long-range wireless transmission in different band) the ends of this link are equipped with transceivers compatible with the ad hoc sensor network to be attacked. After the wormhole link establishment, the malicious nodes capture wireless transmission on one end, sends them through the wormhole link and replays them at the other end (see Figure 2).

WSNs share the security threats of other communication networks, consisting of message interception, modification, and fabrication as well as interruption of communications and operation (DoS), illustrated in Figure1. However, the threats are specifically inherent in WSNs due their special characteristics which enable new forms and combinations of attacks. [Pan 06]

And most proposed protocols to defend against this attack used positioning devices, synchronized clocks, or directional antennas. [Zaw 08] define an new wormhole attack detecting mechanism called Round Trip Time (RTT) and neighbor numbers based wormhole detection mechanism.

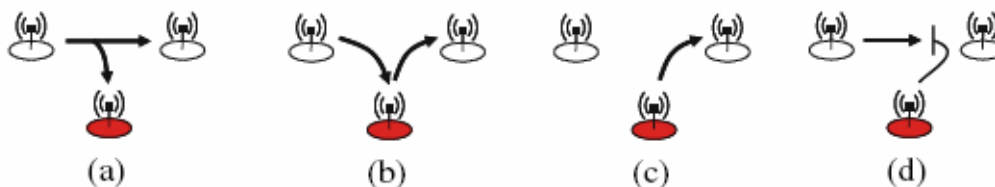


Figure1 : Security threats in WSN communications: (a) interception, (b) modification, (c) fabrication, and (d) interruption [Pan 06]

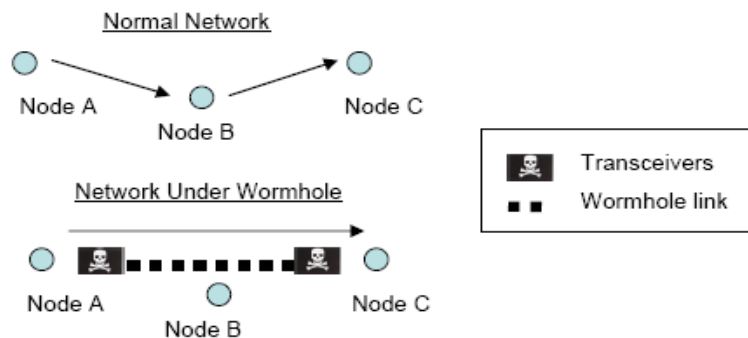


Figure 2: Wormhole establishment. Nodes A and C are false neighbors. Under wormhole attack [Jack 04]

References

- [JFK 07] Jane F. Kinkus «**Science and Technology Resources on the Internet Computer Security**» ,Mathematical Sciences Librarian Purdue University jkinkus@purdue.edu
- [Zaw 08] Zaw Tun and Aung Htein Maw «**Wormhole Attack Detection in Wireless Sensor Networks**» , PWASET volume 36 december 2008 ISSN 2070-3740. Pages 549-554
- [Jack 04] Jackson Kwok «**A Wireless Protocol to Prevent Wormhole Attacks**», A Thesis in TCC 402, Presented toThe Faculty of the School of Engineering and Applied Science University of Virginia, March 23, 2004
- [Pan 06] Panu Hämäläinen, Mauri Kuorilehto, Timo Alho, Marko Hännikäinen, and Timo D. Hämäläinen, «**Security in Wireless Sensor Networks:Considerations and Experiments**» , SAMOS 2006, LNCS 4017, pp. 167–177, 2006.