CS4404 Learning Journal 5

According to (Kalime & Sagar, 2021), there are few common security vulnerabilities in WIFI routing protocols.

* Wormhole Attack:

Malicious nodes create **a shortcut by tunnelling** data packets from one place to another. By retransmitting these packets, attackers disrupt normal routing, jeopardizing data privacy and trustworthiness.

* Hello Flood Attack:

Nodes flood packets to a **specific node, making it more crucial** in the network. Attackers exploit this increased traffic to execute replay attacks or other malicious actions without generating their own traffic.

* Bogus Registration:

Attackers impersonate nodes by giving false information to nearby devices. When packets are forwarded, attackers interrupt nearby devices, potentially causing data manipulation or disruption.

* Rushing Attack:

Nodes quickly establish fake routes between sender and receiver. When genuine requests arrive, attackers reject them, preferring the fake routes established earlier. This causes routing issues and disruptions.

* Black Hole Attack:

A malicious node pretends to offer the shortest route to a destination, attracting traffic but refusing to forward data packets. This results in data loss and disrupts network communication.

These vulnerabilities highlight the susceptibility of wireless routing protocols to various attacks that can disrupt network communication, compromise data integrity, and undermine the overall functionality of the network(Kalime & Sagar, 2021). Implementing robust security mechanisms is crucial to mitigate these threats and ensure the security of wireless networks.

I would like to discussion further on two of the five vulnerabilities.

* **Wormhole Attack**: This attack involves a malicious node recording data packets in one area, tunneling them to another area, and retransmitting them into the network. The attacker creates a shortcut, bypassing normal routing procedures and potentially disrupting communication between legitimate nodes(Kalime & Sagar, 2021). This attack can compromise confidentiality and authenticity, as the attacker can intercept and manipulate data without cooperation from any hosts.
* **Black Hole Attack**: In a Black Hole Attack, a malicious node drops or refuses to forward data packets passing through it, causing data loss and disruption(Kalime & Sagar, 2021). By falsely advertising itself as having the shortest route to a destination node, the attacker attracts traffic, which it then drops or fails to forward. This attack can severely impact the network's performance, leading to data loss and hindering communication between nodes.

These attacks demonstrate the vulnerabilities within wireless routing protocols. They exploit weaknesses in routing mechanisms, allowing attackers to disrupt communication, intercept data, or manipulate routing paths. Implementing robust encryption, authentication, and intrusion detection systems is crucial to mitigate these threats and secure wireless networks against such attacks.

**Reference**

Kalime, S., & Sagar, K. v. (2021). A REVIEW: SECURE ROUTING PROTOCOLS FOR MOBILE ADHOC NETWORKS (MANETs). *Journal of Critical Reviews*, *7*, 8385–8393.