July 2020

MECHANISM TO PROTECT FIELD AREA NETWORKS FROM EAPOL ATTACK

Yajun Xia

Lele Zhang

Chuanwei Li

Li Zhao

MECHANISM TO PROTECT FIELD AREA NETWORKS FROM EAPOL ATTACK

AUTHORS:
Yajun Xia
Lele Zhang
Chuanwei Li
Li Zhao

ABSTRACT

A mechanism is proposed to protect mesh networks from Extensible Authentication Protocol over Local Area Network (EAPOL) attacks in following ways. A Field Network Director (FND) synchronizes a whitelist table to a mesh node periodically, allowing to the mesh node to filter EAPOL messages based on the whitelist table. Further, a supplicant can sign EAPOL messages with its private key, and then a relay node can filter the EAPOL messages base on the signature.

DETAILED DESCRIPTION

In FAN (Field area network: CG-Mesh and WISUN 1.0), the 802.1x EAP-TLS + 802.11i handshake is used for mesh node authentication and key generation. Figure 1 shows the handshake flows.

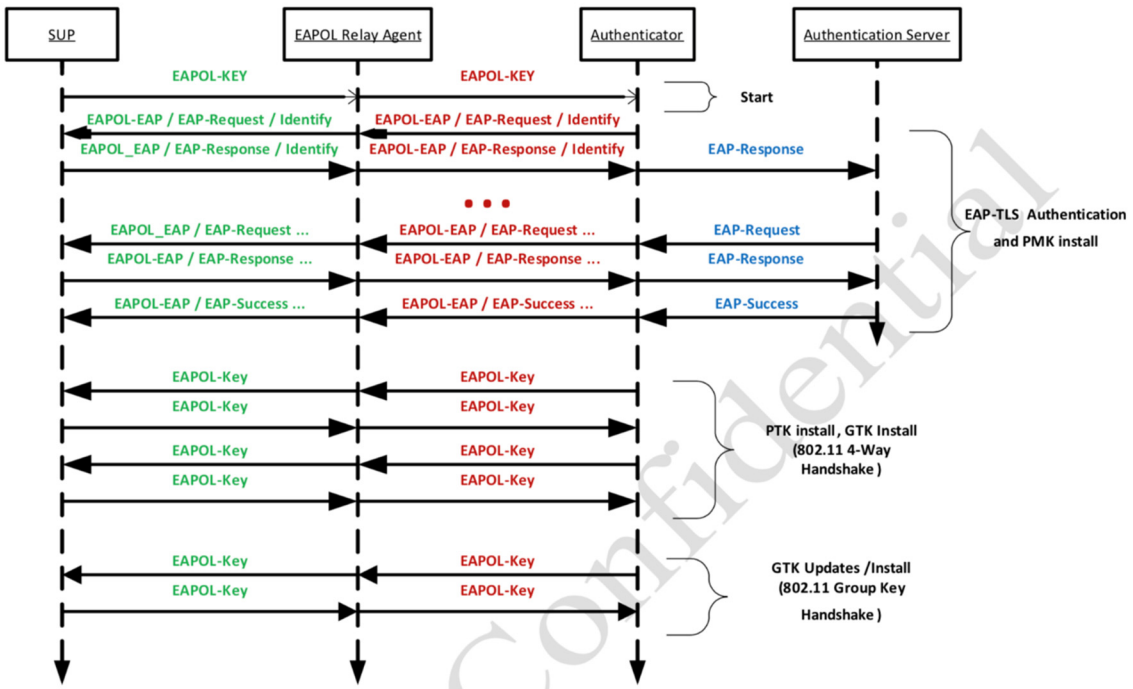

Figure 1

The EAPOL message is not blocked to any supplicant node in a relay node, which means that an EAPOL message from a malicious node could be forwarded to a border router (BR) and radius server.

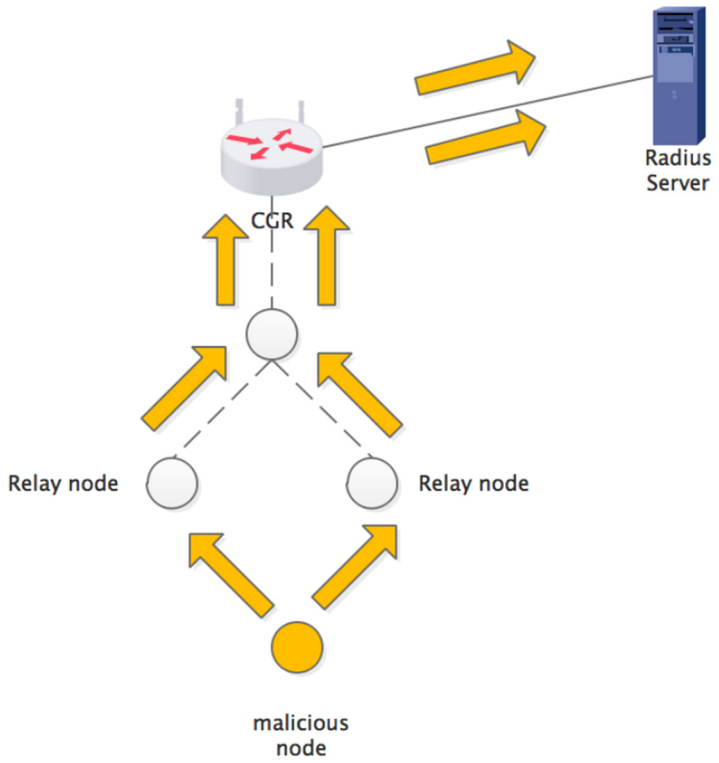

Figure 2

In Figure 2, a malicious node sends EAPOL messages to its relay node. The relay node encapsulates the EAP message as a User Datagram Protocol (UDP) payload, and then sends it hop-by-hop to a Connected Grid Router (CGR) and the radius server for authentication.

A Field Area Network can be considered a Low power and Lossy Network (LLN), since it uses narrow bandwidth transmission (e.g., data rate < ~150kbps), and wireless channel resources can be easy exhausted by extensive EAPOL messaging from a malicious node. The following examples present two different types of EAPOL attacks.

Type 1 EAPOL Attack: The attacker sends forged EAPOL packets with a random source EUI64 address via different relay nodes to the BR/radius server. In this way, the attack is difficult to prevent by a rate limit on the relay node. Figure 1 shows that the EAPOL key message is used to trigger the authentication process.

EAPOL Attack Type 2: The attacker forges the EAPOL Key (start EAPOL) messages by filling different source EUI64 addresses (which are already joined in the mesh network), and then sends them hop-by-hop to the BR/radius server or simply sends the sniffed EAP key message. As a result, the numerous re-authentication EAPOL handshake messages can exhaust the mesh network resources easily and cause network congestion. This is especially so since some EAPOL handshake messages are large (e.g., with certificates encapsulated in perhaps more than 2 Kbytes), which contributes significantly to network congestion.

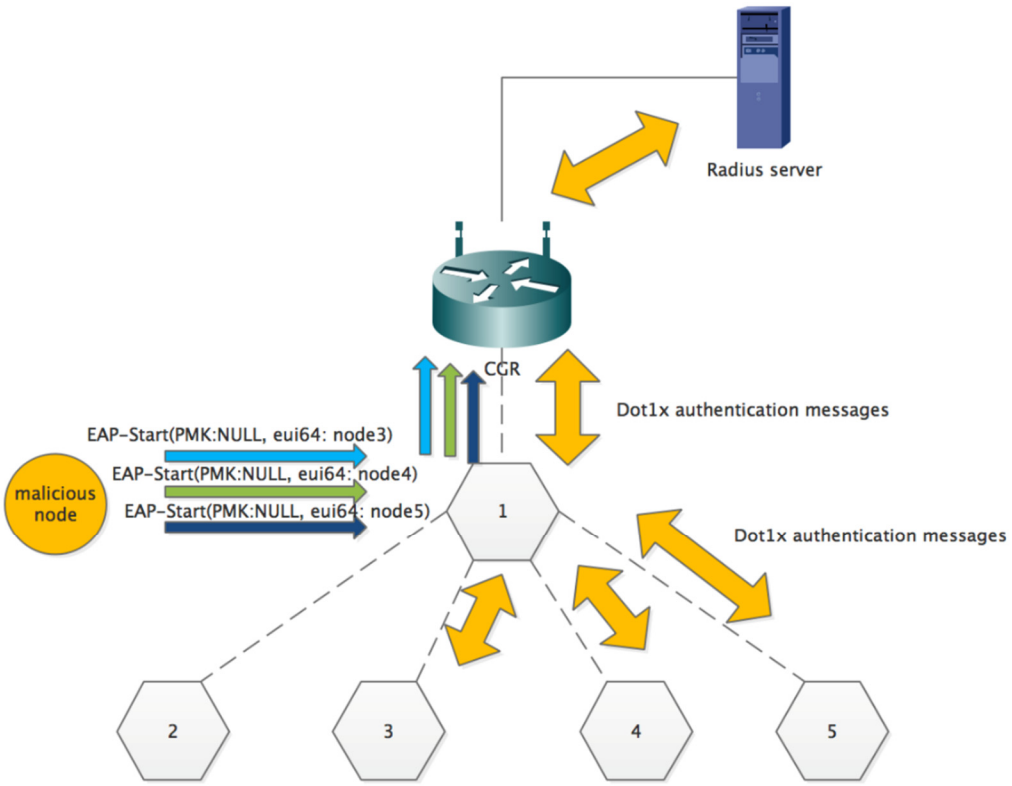

Figure 3

In Figure 3, the malicious attacker forges the EAPOL key messages (herein called mesh EAPOL-start) with all zero PMKID, and fills them with EUI64 of Joined PAN nodes. After the authenticator (CGR) receives the mesh EAP-start messages, the authentication for these nodes will be triggered. As there are certificates (large messages) in some dot1x messages, multi-pairs of dot1x authentication handshakes can exhaust the network resources easily.

The described novel mechanism proposes to protect mesh networks from these types of EAPOL attacks. The mechanism differs from other proposed solutions, such as WIFI networks which use the EAPOL-START frame to trigger Dot1x authentication, and in Cg-Mesh/WISUN, where the EAPOLKEY frame is used to trigger dot1x authentication. Likewise, the proposed solution described herein differs from Wireless Intrusion Prevention System (WIPS) used to detect DoS attacks by tracking the 802.1x authentication state transition and particular attack signatures.

In CG-Mesh network infrastructure, the Field Network Director (FND) will sync the authorized nodes EUI64 address list to a Data Base (DB). When a node tries to join Personal Area Network (PAN), the radius server needs to access the DB to check whether the supplicant node is in the authorized list. If yes, the authentication is successful; otherwise, the authentication fails.

According to one novel aspect of the proposed mechanism, the FND pushes an authorized list to mesh nodes periodically, and a relay node can filter EAPOL traffic from any unknown (i.e., not in the authorized list) supplicant to prevent traffic from a Type 1 EAPOL attack from propagating upward.

According to another novel aspect of the proposed mechanism, the FND inserts the node's online status, and the node and relay node mapping status to the authorized list. The relay node can drop the EAPOL message in the following cases to prevent the EAPOL attack traffic from propagating upward (i.e., a Type 1 EAPOL attack and part of a Type 2 EAPOL attack):

- An EAPOL message from an unknown supplicant.
- An EAPOL message from a supplicant at the status of online, but the relay node is a different node.

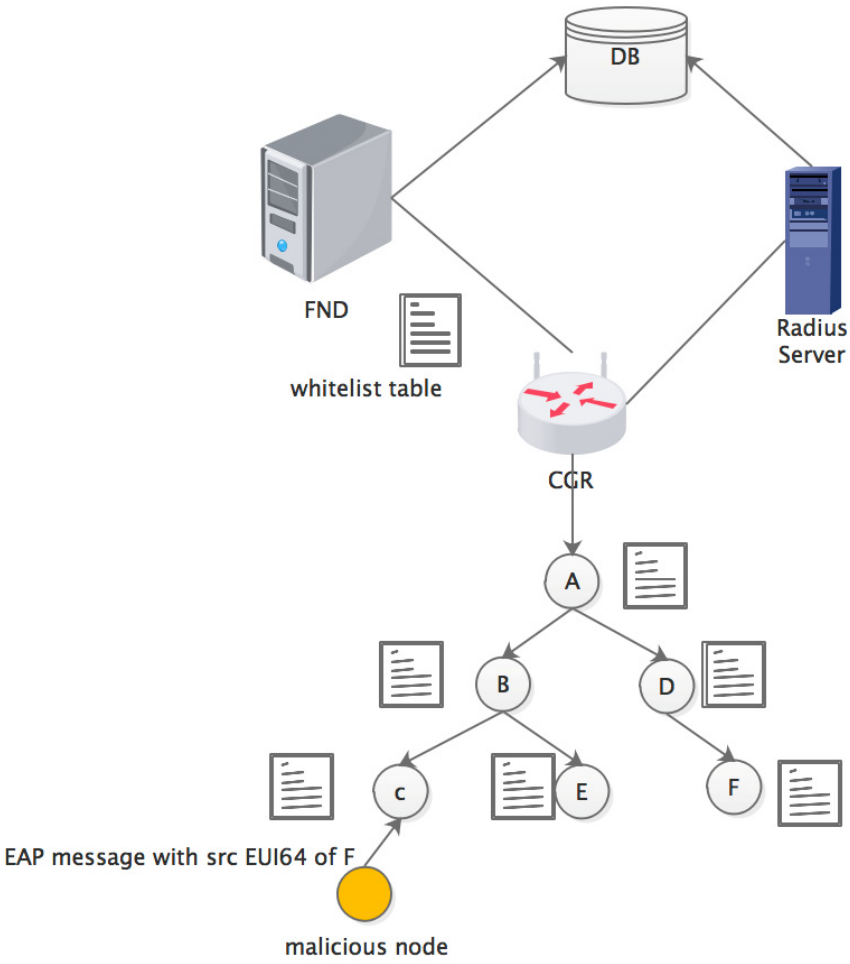

Figure 4

In Figure 4, the FND syncs the authorized list (WhiteList table) to node B after it joins the PAN, and syncs the table periodically. The whitelist table is as follows:

Node	Status	Authorize	Relay Node	PANID
A	Online	Yes	CGR WPAN	1
B	Online	Yes	A	1
C	Online	Yes	B	1
D	Online	Yes	A	1
E	Online	Yes	B	1
F	Online	Yes	D	1

When node C receives the "forged EAPOL message with node F EUI64 address" from the malicious node, it finds that node F is already online bind to relay node D, so then node B drops the message directly.

According to another novel aspect of the proposed mechanism, a supplicant signs an EAPOL message with its private key if it has already join the PAN via same relay point, and the relay node can verify the signature with a cached supplicant's public key to filter Type 2 EAPOL attack traffic from a malicious node.

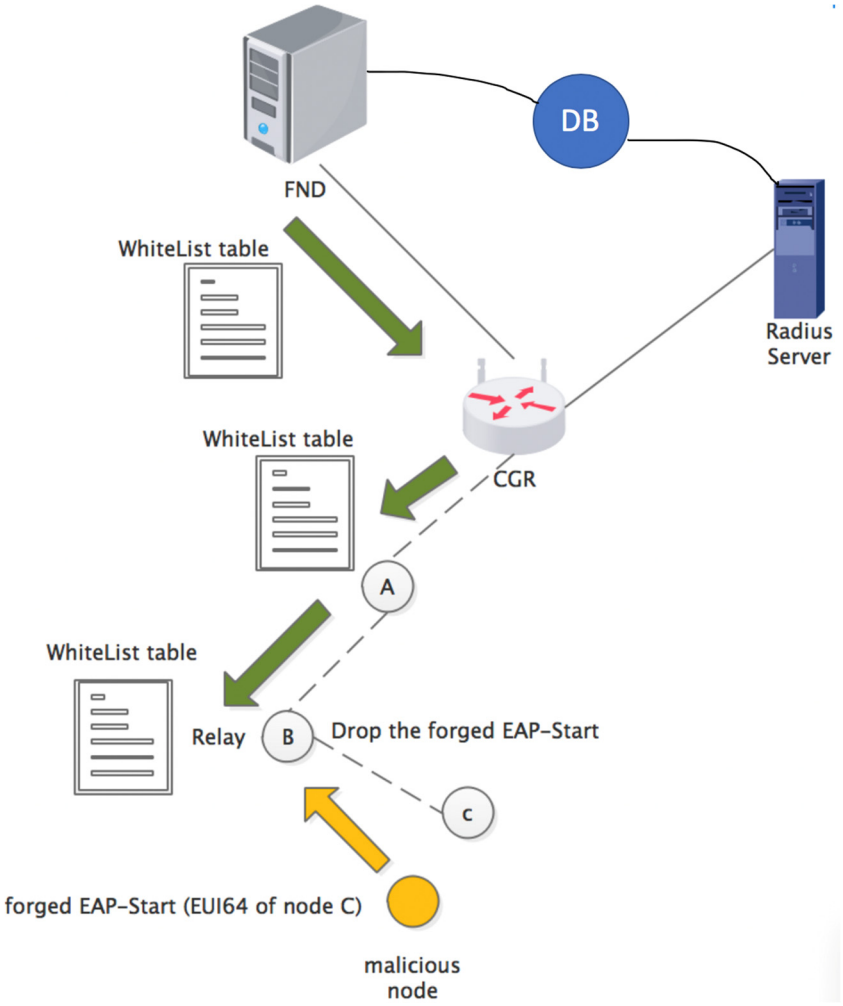

Figure 5

When node B receives the "forged EAP-start" from the malicious node, it finds the supplicant meter is online in the whitelist table and that node B is the relay node for the supplicant, but because there is no signature in the EAPOL message, it drops the EAPOL message. In the case of a replay attack, when node B receives the "replayed EAP-start" from the malicious node, it finds the EAPOL replay counter is an old value, and then it drops the EAPOL message. Because the whitelist table may cost some network resource,

optionally the FND can send the whitelist only to specific nodes (for example all IR510) for attack traffic filtering.