MODULE *Attacker*

EXTENDS *MQTTBase*

CONSTANT *attacker*
CONSTANT *isEncrypted*

VARIABLE
kmsgs,
knows

$attacker\_vars \triangleq \langle kmsgs, knows \rangle$

Attacker

$Eavesdrop \triangleq$
$\land \exists\, a \in agents : Len(network[a]) > 0$
$\land$ LET $x \triangleq$ CHOOSE $a \in agents : Len(network[a]) > 0$ IN
$\land\ kmsgs' = kmsgs \cup \{Head(network[x])\}$
$\land$ UNCHANGED *network*
$\land$ UNCHANGED *knows*

$Intercept \triangleq$
$\land \exists\, a \in agents : Len(network[a]) > 0$
$\land$ LET $x \triangleq$ CHOOSE $a \in agents : Len(network[a]) > 0$ IN
$\land\ kmsgs' = kmsgs \cup \{Head(network[x])\}$
$\land\ network' = [network$ EXCEPT $![x] = Tail(network[x])]$
$\land$ UNCHANGED *knows*

$Replay \triangleq$
$\land\ kmsgs \neq \{\}$
$\land$ LET $des \triangleq$ CHOOSE $a \in agents$: TRUE
$msg \triangleq$ CHOOSE $one \in kmsgs$: TRUE
IN
$\land$ LET $source \triangleq$ CHOOSE $s \in agents : s \neq des$IN
$\land$ LET $fmsg \triangleq [msg$ EXCEPT $!.from = source,\ !.to = des]$IN
$\land\ network' = send(fmsg, fmsg.to)$
$\land$ UNCHANGED *kmsgs*
$\land$ UNCHANGED *knows*

$Forward \triangleq$
$\land\ kmsgs \neq \{\}$
$\land$ LET $msg \triangleq$ CHOOSE $one \in kmsgs$: TRUEIN
$\land$ LET $amsg \triangleq [msg$ EXCEPT $!.from = attacker]$IN
$\land\ network' = send(amsg, amsg.to)$
$\land$ UNCHANGED *kmsgs*
$\land$ UNCHANGED *knows*

$Forge \triangleq$

$\land \neg isEncrypted$
$\land kmsgs \neq \{\}$
$\land knows.clientId \neq \{\}$
$\land \exists\, m \in kmsgs : m.type = CONNECT$
$\land$ LET
$msg \triangleq$ CHOOSE $one \in kmsgs : one.type = CONNECT$
$x \triangleq$ CHOOSE $one \in knows.clientId :$ TRUE
IN
$\land$ LET $fmsg \triangleq [msg$ EXCEPT $!.payload.clientId = x]$IN
$\land \quad kmsgs' = kmsgs \cup \{fmsg\}$
$\land$ UNCHANGED $knows$
$\land$ UNCHANGED $network$

$Resolve \triangleq$
$\land \neg isEncrypted$
$\land kmsgs \neq \{\}$
$\land$ LET $msg \triangleq$ CHOOSE $one \in kmsgs :$ TRUEIN
$\land \quad knows' =$ CASE $msg.type = CONNECT \to [knows$ EXCEPT $!.clientId = @ \cup \{msg.payload.clientId\}$
$\square msg.type = PUBLISH \to [knows$ EXCEPT $!.msgID = @ \cup \{msg.packetID\},\ !.topic = @$
$\square msg.type = SUBSCRIBE \to [knows$ EXCEPT $!.topic = @ \cup \{msg.topic\}]$
$\square$OTHER $\to knows$
$\land$ UNCHANGED $network$
$\land$ UNCHANGED $kmsgs$

$IoTDeviceAttack \triangleq$
$\land knows' = [knows$ EXCEPT $!.clientId = @ \cup clients]$
$\land$ UNCHANGED $network$
$\land$ UNCHANGED $kmsgs$

$AttackerInit \triangleq$
$\land kmsgs = \{\}$
$\land knows = [$
$clientId \mapsto \{\},$
$topic \mapsto \{\},$
$msgID \mapsto \{\}$
$]$

$AttackerAction \triangleq$
$\lor Eavesdrop$
$\lor Intercept$
$\lor Forward$
$\lor Replay$
$\lor Resolve$
$\lor Forge$
$\lor IoTDeviceAttack$