Un enfoque basado en la confianza para el intercambio de datos en el entorno MQTT

Liang Chen , Stilianos Vidalis y Su Yang†
Departamento de Ciencias de la Computación, Universidad de Hertfordshire, Hatfield, Reino Unido
†Departamento de Ciencias de la Computación, Universidad de Swansea, Swansea, Reino Unido

Resumen—El Internet de las cosas (IoT) se considera una red gigante de dispositivos conectados que recopilan datos y los comparten entre sí. Se han producido grandes avances en los estándares y protocolos de IoT que permiten a los dispositivos de IoT intercambiar datos de una manera estructurada y significativa. El transporte de telemetría de colas de mensajes (MQTT) es uno de esos desarrollos que está recibiendo una amplia adopción para aplicaciones industriales. Está diseñado como un protocolo de mensajería liviano basado en el modelo de publicación-suscripción mediante el cual los clientes publican mensajes a un corredor que es responsable de distribuir los mensajes a los clientes suscritos. MQTT a menudo se implementa en un entorno hostil en el que los dispositivos y corredores de IoT son vulnerables a los ataques. Si bien la seguridad para MQTT ha recibido gran atención, no aborda adecuadamente los problemas de autorización dentro de un entorno MQTT descentralizado.

El trabajo existente adopta enfoques basados en políticas para regular el intercambio de datos entre múltiples corredores, lo que creemos que es poco probable que se amplíe bien. En este artículo proponemos un enfoque basado en la confianza que puede incorporarse fácilmente a la implementación existente del corredor MQTT. Introducimos una forma de calcular la calificación de confianza de los corredores y desarrollamos dos medios para utilizar las calificaciones de confianza para controlar el flujo de datos entre múltiples dominios de corredores. Nuestro enfoque es capaz de detectar y bloquear clientes y corredores maliciosos para que no envíen mensajes falsos o maliciosos al sistema.

I. INTRODUCCIÓN

El Internet de las Cosas (IoT) representa la gran cantidad de dispositivos que se conectan a Internet para intercambiar información en tiempo real. En general, cualquier dispositivo que sea capaz de enviar y recibir datos a través de una red se considera un dispositivo IoT. Esto incluye ordenadores portátiles, teléfonos inteligentes, televisores, termostatos, pero también sensores, microcontroladores y actuadores con recursos limitados. Las soluciones de IoT están permitiendo nuevas formas de mejorar la eficiencia, la flexibilidad y la productividad, lo que se desprende de la palabra de moda "inteligente" que aparece al frente de áreas clave: ciudad, carreteras, hogares, agricultura, salud y depósitos logísticos.

Se han producido grandes avances en los estándares y protocolos de IoT que permiten a los dispositivos de IoT intercambiar datos de una manera estructurada y significativa. Uno de los protocolos más adoptados en IoT es el transporte de telemetría de colas de mensajes (MQTT) [1]. MQTT es un protocolo de mensajería ligero y escalable, diseñado específicamente para conectar una gran escala de dispositivos con recursos limitados. Funciona según los principios del modelo de publicación-suscripción para desacoplar el remitente del mensaje (editor) del receptor del mensaje (suscriptor). En cambio, un tercer componente, llamado intermediario, filtra todos los mensajes entrantes de los editores y los distribuye correctamente a los suscriptores.

Cuantos más dispositivos estén conectados a Internet, más atractivos se volverán los datos para los ciberataques. El MQTT

El protocolo especifica algunos mecanismos de seguridad como la autenticación de usuarios y dispositivos, la autorización entre clientes y el broker, la integridad y confidencialidad de los paquetes de mensajes, pero la forma de implementar estos mecanismos depende de los desarrolladores de aplicaciones [1]. En este artículo hemos examinado específicamente las soluciones de autorización proporcionadas por las implementaciones modernas de los brokers MQTT1. Resulta que las listas de control de acceso y OAuth2.0 se encuentran entre las más populares. Sin embargo, sus pautas de implementación introducen estas soluciones de autorización solo para el contexto de un único corredor, por lo que no es obvio cómo se pueden extender a un entorno MQTT descentralizado donde varios corredores se conectan entre sí para compartir datos. Normalmente, dicho entorno presenta las siguientes características:

- Los dispositivos IoT con recursos limitados que se ejecutan en entornos hostiles son vulnerables a ataques de seguridad, como convertirse en malware que difunde información falsa en la red IoT.
- Los datos a menudo se comparten entre dispositivos que pertenecen a diferentes dominios de seguridad controlados por diferentes agentes locales. En otras palabras, un dispositivo puede compartir datos con otro que no se conoce de antemano.

El trabajo existente utiliza un enfoque basado en políticas (ya sea imponiendo políticas de flujo de información [2] o políticas de autorización basadas en atributos junto con las preferencias del usuario [3]) para regular el intercambio de datos en un entorno MQTT tan descentralizado, que creemos que es poco probable que se amplíe. bien y sufren la carga administrativa de las políticas. La gestión de fideicomisos parece ser un enfoque natural, pero hasta donde sabemos, aún no se ha propuesto. Estas consideraciones son el foco de este artículo. Más específicamente, resumimos nuestras contribuciones de la siguiente manera:

- Tomamos el principio de OAuth2.0 para introducir el concepto de token de autorización, que es un conjunto de permisos otorgados a dispositivos IoT para publicar y suscribirse a temas de mensajes. Este enfoque de autorización basado en tokens es compatible con las implementaciones MQTT existentes. • Proponemos un modelo de confianza subjetiva para calcular la confiabilidad de los brokers en términos de la adecuada gestión de sus dispositivos y políticas de autorización. Cuando un corredor recibe una solicitud de publicación de mensajes junto con su token de autorización, determina si acepta el token evaluando la confiabilidad de los corredores que firmaron el token.

1MQTT Software: https://mqtt.org/software/

• Proponemos dos formas de evaluar la aceptación de un token de autorización en toda la red de corredores, reflejando diferentes grados de seguridad que podemos aplicar para el entorno MQTT descentralizado.

II. FONDO

En esta sección describimos materiales de referencia relevantes sobre MQTT y la evaluación de confianza subjetiva.

R. MQTT

MQTT es el protocolo de mensajería más popular para Internet de las cosas (IoT) y se utiliza en una amplia variedad de industrias que van desde la automoción, el hogar inteligente, la logística hasta la fabricación. Emplea la arquitectura de publicación-suscripción para mensajería e intercambio de datos entre dispositivos de IoT. Un dispositivo IoT (cliente denominado) envía (publica) mensajes sobre un tema a un servidor (broker denominado) que es responsable de distribuir los mensajes a los clientes que se suscribieron previamente al tema determinado. La figura 1 muestra una topología en estrella de la arquitectura de publicación-suscripción MQTT en la que los clientes están desacoplados entre sí y el intermediario maneja la conexión entre ellos.

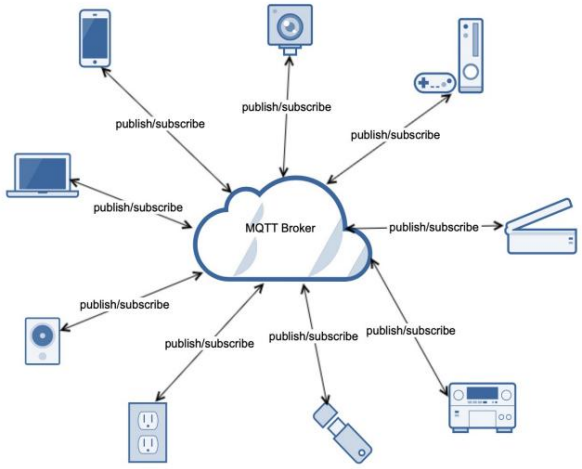

Fig. 1. Arquitectura de publicación-suscripción MQTT

Un concepto interesante en MQTT es el filtro de temas, que es una cadena UTF-8 que el intermediario utiliza para filtrar mensajes para cada cliente conectado. El filtro de temas consta de uno o más niveles de temas y cada nivel de tema está separado por una barra diagonal. Un ejemplo de filtro de tema es inicio/ + /dormitorio/#, donde + y # son comodines que cubren un solo nivel y varios niveles respectivamente. Tenga en cuenta que un cliente puede utilizar comodines para suscribirse a varios niveles de temas. Por ejemplo, si un cliente está suscrito a los temas: casa/ + /dormitorio/#, significa que puede escuchar todos los mensajes relacionados con el dormitorio en todos los pisos (+) y todo lo que hay allí (#). Al publicar mensajes, un cliente puede enviar un mensaje (21,5 °C) bajo un tema específico (casa/segundo piso/dormitorio/temperatura) que el corredor utiliza para reenviar el mensaje a todos los clientes suscritos.

Es importante observar que los clientes de publicación no pueden utilizar caracteres comodín en los nombres de los temas que publican.

MQTT proporciona algunas características importantes, incluida la Calidad de servicio (QoS), que brinda a los clientes el poder de elegir un nivel de servicio que coincida con la confiabilidad de su red y la lógica de aplicación. El intermediario de mensajes gestiona la retransmisión de mensajes y garantiza la entrega según los niveles elegidos por los clientes. Puede consultar un estudio detallado de las características proporcionadas por la última versión de MQTT (MQTT v5.0) en el documento estándar [1].

B. Modelo de confianza

Si bien existen muchos modelos de confianza más complejos, adaptamos el enfoque basado en la lógica subjetiva ampliamente utilizado de Josang [4], que es un modelo relativamente sencillo basado en principios bayesianos.

Una opinión que tiene un agente x sobre el agente y respecto al tema i es una tupla $\omega = \alpha_{xy:i}, \beta_{x\,y:i}, \gamma_{x\,y:i}$ [0, 1]. Los valores de $\alpha = 1$ y $\delta_{xy:i}$ $\alpha_{xy:i}, \beta_{xy:i}, \gamma_{xy:i}$ representa los grados de creencia, incredulidad e incertidumbre con respecto a la proposición de que el agente y se comportará como x espera con respecto al problema i. El parámetro de tasa base $\delta_{xy:i}$ representa el grado de confianza a priori que el agente x en cuestión tiene sobre y, antes de que se haya adquirido cualquier evidencia directa.

Las opiniones se forman y actualizan mediante valoraciones de rentabilidad pasada: $r_{x\,y:i}$ binarias, $s_{x\,y:i}$ siendo las experiencias positivas y las valoradas como negativas. Entonces se puede calcular la opinión de un agente $\omega_{x\,y:i}$ como $\alpha_{xy:i} = r_{x\,y:i}/(r_{x\,y:i}+s_{x\,y:i}+2)$; $\beta_{xy:i} = s_{x\,y:i}/(r_{x\,y:i}+s_{x\,y:i}+2)$; y $\gamma_{x\,y:i} = 2/(r_{x\,y:i}+s_{x\,y:i}+2)$. Para una opinión inicial sin evidencia, por lo tanto, $\alpha_{x\,y:i} = 0$, $\beta_{x\,y:i} = 1$, y $\delta_{x\,y:i}$ es típicamente establecido automáticamente en 0,5. Dada una opinión calculada sobre y con respecto a i, se puede obtener una calificación de confianza de un solo valor, que puede usarse para clasificar y comparar individuos: $\tau_{x\,y:i} = \alpha_{x\,y:i} + \delta_{x\,y:i} \cdot \gamma_{x\,y:i}$.

III. NUESTRO ENFOQUE BASADO EN LA CONFIANZA

A. Fichas de autorización

Un cliente MQTT puede hacer básicamente dos cosas después de conectarse a un corredor: publicar mensajes y suscribirse a temas. Sin la autorización adecuada, cada cliente autenticado puede publicar y suscribirse a todos los temas disponibles, incluidos los clientes maliciosos. Dado que MQTT a menudo se implementa en un entorno de comunicación hostil, el estándar recomienda la provisión de un mecanismo de autorización que sea capaz de restringir a los clientes a publicar y suscribirse únicamente a temas autorizados.

Los clientes MQTT pueden ser dispositivos con recursos limitados y tener una potencia de cálculo limitada, por lo que es necesario implementar un mecanismo de autorización por parte del intermediario. Tal mecanismo proporcionaría una decisión de autorización evaluando una solicitud de acceso con respecto a una política de autorización. Para definir políticas de autorización, utilizamos un enfoque basado en capacidades que ha sido ampliamente estudiado para la autorización en el contexto de IoT [5]. Además, la última implementación de autenticación y autorización para MQTT [6] aboga por la

uso de OAuth 2.02 , que es una autorización basada en capacidad protocolo de delegación.

Seguimos el principio de OAuth 2.0 para asumir la existencia de un servidor de autorización (AS) que es responsable de registrar clientes y gestionar las políticas de autenticación y autorización en nombre de un corredor. Cuando un cliente se registra con AS, AS emitirá un token de autorización (AT) que define un conjunto de permisos otorgados al cliente. En otras palabras, un token de autorización simplemente enumera todas las solicitudes autorizadas con respecto al cliente. En este documento no nos centramos en cómo el AS autentica a un cliente para que emita un AT, lo que depende de muchos factores diferentes, como la identificación del cliente, la confiabilidad, la ubicación del cliente, las políticas del propietario del cliente, etc. La figura 2 muestra la autenticación. y flujo de autorización para un cliente que se conecta a un corredor. Para simplificar nuestras discusiones posteriores sobre el caso de múltiples corredores, decimos que, de ahora en adelante, AT es emitido por un corredor en lugar de AS.

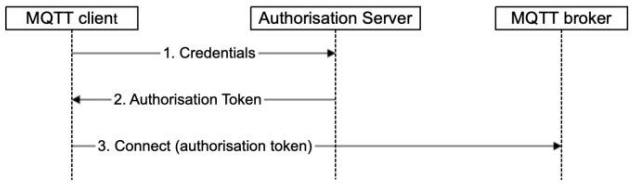

Fig. 2. Flujo de autorización del cliente en MQTT

Sea F un conjunto de filtros de temas. Dados dos filtros de temas, f, f′ F, escribimos f f si los temas contenidos en f es un subconjunto de temas contenidos en f. Por ejemplo, sean f = hogar/ + /dormitorio/# y f = hogar/# , tenemos f f Sea C un conjunto de clientes. Definimos un AT como una tupla b, c, S, Fp, Fs , donde b es un corredor que emite el AT, c es el cliente que recibe el token, S es un conjunto de corredores que firman digitalmente el token y Fp es un conjunto de filtros de temas que c puede publicar y Fs es un conjunto de filtros de temas a los que c puede suscribirse. En un entorno de un solo corredor, S = {b}, lo que significa que AT es emitido y firmado por un único corredor b, pero la estructura que definimos es para un caso general en el que AT puede ser firmado por múltiples corredores cuando pasa por la red de corredores. . Estudiamos el caso general en la siguiente sección. Tomemos ahora un ejemplo de AT = b, c, {b}, Fp, Fs , donde Fs = {casa/primer piso/#} y Fp = {casa/planta baja/cocina}, lo que sugiere que el cliente c es autorizado a publicar un mensaje sobre el tema (casa/planta baja/cocina) y a suscribirse a todos los temas bajo casa/primer piso.

Dada una solicitud del cliente c para publicar un mensaje de tema f:m, denotado por reqp (c, f:m), decimos que el corredor b concede reqp (c, f:m) si c tiene un AT = b , c, {b}, Fp, Fs y existe f Fp tal que f = f cliente c para suscribirse a los temas f, ′. Ante una solicitud de denotado por reqs (c, f), decimos que se conceden reqs (c, f) por el corredor b si c posee un AT = b, c, {b}, Fp, Fs y existe ff f ′ Fs tal que ′.

B. Mensajería a través de una red de intermediarios

En una implementación compleja de IoT, los corredores se conectan entre sí para formar una red de corredores, con el fin de facilitar el intercambio de datos entre clientes de diferentes dominios. Nuestro enfoque para controlar el intercambio de datos a través de una red de corredores es simple y requiere pocos cambios en la especificación MQTT original.

La figura 3 muestra un ejemplo de una red de corredores en la que los nodos rojos representan clientes y los nodos verdes representan corredores. El corredor b1 se conecta a dos corredores b2 y b3, y b3 se conecta a b4 y b5, lo que se refleja como bordes en la red.
Suponemos que cada cliente sólo puede registrarse con un corredor a la vez. Después de autenticarse con el corredor, el cliente recibe un AT de ese corredor que define los temas a los que puede publicar y suscribirse. Cuando un cliente publica un mensaje sobre un tema, es posible que no sepa que el corredor compartirá el mensaje con clientes de otros dominios, porque los clientes están autorizados a publicar un mensaje sobre un tema, sin tener que ver con los receptores. Ese es el principio de desacoplamiento del modelo de publicación-suscripción.

Para dos corredores conectados, se registran entre sí y reciben un AT entre sí. Por ejemplo, cuando b2 se registra con b1, b1 trata a b2 como uno de sus clientes y emite un AT que define los temas a los que b2 puede suscribirse, que tiene la forma b1, b2, S, , Fs . Sería la misma semántica cuando b1 se registra con b2. Tenga en cuenta que el AT que recibe un corredor solo contiene permisos de suscripción, no de publicación, esto se debe a que la función del corredor es administrar la autorización y reenviar mensajes a sus clientes autorizados.

Dado un intermediario b, hemos configurado un flujo de mensajes bidireccional a través de b. Uno es el de los corredores vecinos que reenvían mensajes "entrantes" a los que b está suscrito. La otra forma es que b reenvía mensajes "salientes" a sus corredores vecinos sobre los temas a los que se han suscrito. Con nuestro enfoque, un mensaje puede pasar de un corredor a otro, permitiendo las comunicaciones de clientes en diferentes dominios.

Ahora usamos el ejemplo de la Fig. 3 para explicar cómo cada corredor b toma una decisión sobre si distribuir un mensaje entrante a sus clientes y corredores suscritos. Cuando el corredor b1 recibe una solicitud de publicación de un mensaje de uno de sus clientes c, compara la solicitud con el token AT en poder de c. Si el token es válido y permite la solicitud, el mensaje se reenvía a sus clientes suscritos en b1. Tenga en cuenta que estas solicitudes se evalúan de acuerdo con el mecanismo que definimos en la Sección III-A. Si el corredor b2 está suscrito al tema asociado con el mensaje, b1 reenvía la solicitud junto con el AT a b2. El corredor b2 trata la solicitud y AT como si vinieran de sus propios clientes, pero realiza operaciones específicas para verificar la aceptación de AT de la siguiente manera: 1) Evalúa la validez de AT verificando la firma de b1

en la ficha;

2) Calcular la calificación de confianza de confianza (b1, b2) que representa la opinión de b2 sobre la confiabilidad de b1 en términos de la gestión adecuada de sus políticas de autorización;

2OAuth 2.0: https://oauth.net/2/

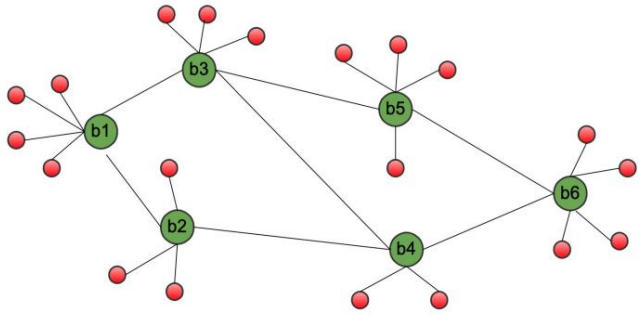

Fig. 3. Ejemplo de una red de corredores

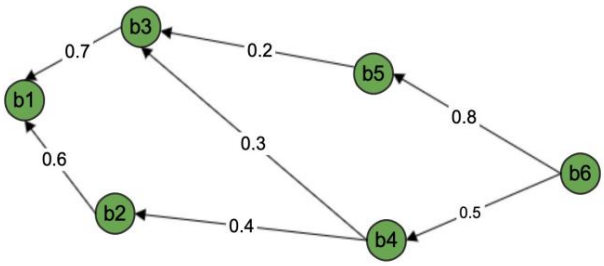

Fig. 4. Ejemplo de gráfico ponderado

3) Si confianza (b1, b2) π, donde π es un umbral de confianza definido globalmente por el sistema, entonces b2 firma el AT. Esto actúa como un "introductor" de b1 a otros corredores conectados a b2 ; 4) Distribuir el mensaje a su cliente suscrito y reenviar la solicitud y el AT actualizado a sus intermediarios conectados b4 distintos de b1.

Supongamos que el corredor b4 también está suscrito al mensaje. Cuando b4 recibe la solicitud y AT, realiza las mismas operaciones descritas anteriormente, pero si confianza (b2, b4) < π, ¿ b4 debería rechazar la solicitud o aceptarla y reenviarla más abajo en la red?

Antes de explorar esta cuestión, primero averigüemos cómo evaluar la confiabilidad de los corredores.

C. Calificaciones de confianza informáticas

La confiabilidad de los corredores es un elemento fundamental para determinar si una AT es aceptable. Nuestro enfoque para evaluar la confiabilidad de los corredores es capaz de detectar y eliminar corredores maliciosos o comprometidos en una red.

La calificación de confianza de un corredor bi por corredor bj , denotada por confianza (bi , bj), representa cuánto confía bj en bi para gestionar adecuadamente la autorización de sus clientes. Esto se refleja en las interacciones previas de bj con bi con respecto a la "calidad" de los datos Let se reciben de bi . ser un historial de eventos de publicación de mensajes realizados por el corredor bj , cuyos miembros son la forma de bi , m, f , lo que representa que un mensaje m sobre el tema f fue autorizado para ser reenviado desde el corredor bi .

Dada una historia H j, el corredor bj puede evaluar los eventos históricos: Ej : H j → {pos, neg}. Por lo tanto, a través de esta función, un evento observado bi , m, f H ji puede alimentar actualizaciones de confianza positivas o negativas. Si b2 considera que el mensaje m es de buena calidad, lo que significa que de hecho era la información que se espera que reciba bj , entonces resulta en una actualización positiva, mientras que en caso contrario se obtiene una actualización negativa. Uno de nuestros trabajos futuros priorizados es especificar cómo funciona Ej , lo cual depende de muchos factores. Uno obvio puede ser la retroalimentación directa de los clientes de bj ' que se suscribieron al mensaje del tema f:m. Estos comentarios pueden ser proporcionados por los propietarios cuyos dispositivos IoT (clientes) se implementaron en el corredor bj .

Dada la función Ej , nos gusta capturar una situación en la que la confianza aumenta gradualmente con una experiencia positiva en las interacciones y disminuye significativamente con una experiencia negativa. Para cada h H j tal que Ej (h) = pos, tenemos r + 1. Cuando $r_i^j = r_i^j$ existe h H j tal que Ej (h) = neg, hacemos $s_i^j = s_i^j$ jj + μ, donde μ Z y μ > 1. La elección de μ hace que s_i^j crece más rápido cuando ocurre una interacción negativa. El corredor bj + δ jj calcular periódicamente la confianza (bi , bj) = α donde γ_i^j se calculan en i , c i , δj función de r i j y si yo . puede a jj

D. Tomar decisiones

En la Sección III-B, no hemos presentado explícitamente cómo un corredor toma una decisión sobre si una solicitud de publicación y AT son aceptables. Un enfoque sencillo es que el corredor verifique si sus corredores vecinos han firmado el token y evalúe el puntaje de confiabilidad de estos corredores. Formalmente, construimos un gráfico ponderado acíclico dirigido G = B, E, T , donde B es un conjunto de corredores y T : E → [0, 1] es una función que asigna bordes dirigidos a su calificación de confianza. Dado un borde e = (b, b′) E, se dice que b es adyacente a b y se dice que b es adyacente a b. Dado a , b) E} ,a , , , corredor b B, escribimos −→A(b) = {b B : (b representan un conjunto de corredores que son adyacentes a b. Esencialmente, T(e) = confianza(b, b′) calcula la calificación de confianza dinámica de b por b . Dado un AT = b, c, S, Fp, FS , cada corredor B, quien ′) tal recibe AT, lo aceptaría si existiera b b −→A(b S y confiara(b “, b′) π, y rechazarlo en caso contrario. Eso b simplemente significa que el corredor b aceptaría el token AT solo si uno de sus vecinos confiables ha firmado el t

En otras palabras, el corredor b solo confía en los presentadores que se conectan directamente con ella y tienen interacciones positivas con ella en términos de intercambio de mensajes autorizados. Este enfoque es intuitivamente razonable pero puede resultar demasiado restrictivo para la difusión de mensajes en el entorno MQTT.

A continuación presentamos un enfoque menos restrictivo que permite a un corredor reenviar mensajes a otros corredores sin la necesidad de firmar el AT. Introducimos un umbral local θj [0, 1] cuyo valor está determinado por el corredor bj , que representa el valor mínimo de confianza para que bj acepte el AT.

Por supuesto, requerimos que θj π, lo que significa que el corredor bj puede aceptar el token pero no desea firmarlo. Dado un gráfico ponderado acíclico dirigido G = B, E, T , una ruta entre b1 y bn es una secuencia de corredores b1, b2 ,. . . , bn tal que cada par consecutivo (bi , bi+1) E y 1 i < n. Luego definimos una calificación de confianza de b1 por bn a lo largo del camino b1 ,. . . , bn es el promedio de todas las calificaciones de confianza en el borde a lo largo del camino,

eso es $\prod_{yo=1}^{n-1}$ confianza(i, i + 1)/n − 1, denotada por confianza(b1, . . . , bn). Tenga en cuenta que puede haber muchos caminos entre b1 y bn, cada uno de los cuales puede tener diferentes calificaciones de confianza. Una o más de estas rutas tienen la calificación mínima de confianza, que llamamos ruta menos confiable. Dado que un AT = b1, c, S, Fp, Fs llega al corredor bn, bn aceptaría AT si existe b S tal que, entre todos los caminos de b a bn, el camino b menos confiable, . . . , bn cuya calificación confía(b, . . . , bn) θn. En otras palabras, cuando bn recibe el token AT, determina si lo acepta comprobando si hay un corredor b que firma el token y si la ruta mínima de calificación de confianza de b a bn supera el umbral θn. La razón para que bn verifique el camino menos confiable desde b es enfatizar la seguridad, lo que significa que cuando bn decide aceptar el token, se asegura de que no exista un camino de b a bn cuya calificación de confianza sea menor que el umbral. θn. Por supuesto, podemos imponer además una condición, como PGP [7], que requiere al menos dos o tres firmantes cuyo camino menos confiable hacia bn esté por encima de θn.

Tomemos el ejemplo de la Fig. 4. Supongamos que b6 recibe una ficha AT = b1, c, {b1, b2, b3}, Fs, Fp y θ6 = 0,5. b6 decide si acepta el AT mirando los caminos menos confiables de b1, b2 y b3. Supongamos que b6 evalúa primero el camino b2, b4, b6 cuya confianza (b2, b4, b6) = 0,45, que es menor que θ6. Luego evalúa dos caminos desde b3, es decir , b3, b4, b6 y b3, b5, b6. Podemos ver que el camino menos confiable entre b3 y b6 es b3, b4, b6 y la calificación de confianza para este camino confianza (b3, b4, b5) = 0,4, que es menor que θ6. Finalmente , b6 vuelve a mirar los caminos desde b1. Hay tres caminos entre b1 y b6: b1, b2, b4, b6 y b1, b3, b4, b6 y b1, b3, b5, b6, dos de los cuales son los caminos menos confiables, es decir, b1, b2. , b4, b6 y b1, b3, b4, b6. La calificación de confianza de las dos rutas es la misma, es decir, 0,5 equivale a θ6. Por tanto, b6 aceptaría el token y distribuiría el mensaje a sus clientes suscritos.

Tenga en cuenta que el problema de verificar la aceptación del token por parte de un corredor se reduce esencialmente a calcular las rutas menos confiables desde los firmantes del token hasta el corredor.

Intuitivamente, ningún corredor tiene información completa sobre la calificación de confianza de todos los bordes de la red. En cambio, cada corredor comienza con sólo el conocimiento de las calificaciones de confianza de sus propios corredores directamente conectados. Luego, a través de un proceso iterativo de cálculo e intercambio de información con sus corredores vecinos, un corredor calcula gradualmente la ruta menos confiable hacia un destino o conjunto de destinos (firmantes de tokens).

Estas son las características del algoritmo de enrutamiento Distancia-Vector (DV) [8] que se basa en la célebre ecuación de Bellman-Ford, a saber: dx(y) = minv{c(x, v) + dv(y)}, donde el minv en la ecuación se toma sobre todos los vecinos de x. Utilizamos el algoritmo DV para calcular las rutas menos confiables de manera asincrónica e iterativa, con el fin de tomar decisiones efectivas para la aceptación de tokens.

IV. OBSERVACIONES FINALES

Estamos realizando una evaluación experimental de nuestros enfoques basados en la confianza, que se divide en dos partes. La primera parte es implementar los mecanismos que proponemos sobre una base Corredor MQTT de código abierto (Eclipse Mosquitto3). La segunda parte consiste en simular un entorno de evaluación en el que clientes y corredores presentan perfiles diferentes, como corredores honestos, maliciosos e incluso coludidos que manipulan sus calificaciones de confianza.

Al completar una cantidad razonable de nodos para la red de corredores, la simulación brindaría una evaluación exhaustiva de la efectividad de nuestro enfoque basado en la confianza.

En términos de trabajos relacionados, existe un conjunto considerable de estudios sobre la propuesta de modelos de seguridad para preservar la confidencialidad de los sistemas generales de middleware de publicación-suscripción [9]. Uno de los trabajos cerrados al nuestro se debe a Pesonen et al. [10] que utilizan los certificados de autorización SPKI para propagar la autorización en diferentes dominios. Creemos que el descubrimiento de la cadena de certificados SPKI/SDSI es un caso especial de nuestro enfoque, es decir, encontrar un camino a lo largo de un conjunto de intermediarios, todos los cuales deben ser firmantes de un token, pero que no requieren cálculo ni evaluación de confianza explícitos. entre los corredores. En otras palabras, nuestro enfoque es más flexible y capaz de detectar clientes y corredores comprometidos evaluando su confiabilidad. Otra línea de trabajo relacionada con la nuestra es el estudio de la autorización para MQTT [2], [3] y su aplicación criptográfica [11], ninguno de los cuales, sin embargo, incorpora el concepto de confianza para un entorno MQTT totalmente descentralizado.

En este documento, tomamos esta iniciativa para desarrollar un enfoque de confianza flexible que cumpla con el estándar MQTT y las implementaciones disponibles. En particular, proporcionamos un medio para calcular una calificación de confianza entre dos corredores vecinos y exploramos dos formas de utilizar estas calificaciones de confianza para controlar el intercambio de datos en una red de múltiples corredores.

REFERENCIAS

[1] “MQTT versión 5.0”, OASIS, Estándar, marzo de 2019.

[2] JCF Carranza y PWL Fong, “Políticas de intermediación y monitores de ejecución para middleware de IoT”, en Actas del 24º Simposio ACM sobre modelos y tecnologías de control de acceso, 2019, págs.

[3] P. Colombo, E. Ferrari y ED Tumer, “Regulación del intercambio de datos en entornos MQTT”, Journal of Network and Computer Applications, vol. 174, pág. 102907, 2021.

[4] A. Jøsang, R. Hayward y S. Pope, “Confiar en el análisis de redes con lógica subjetiva”, en Actas de la 29ª Conferencia de Ciencias de la Computación de Australasia, 2006, págs.

[5] S. Gusmeroli, S. Piccione y D. Rotondi, “Un enfoque de seguridad basado en capacidades para gestionar el control de acceso en Internet de las cosas”, Mathemat-ical and Computer Modelling, vol. 58, núm. 5-6, págs. 1189-1205, 2013.

[6] M. Michaelides, C. Sengul y P. Patras, “Una evaluación experimental de la autenticación y autorización MQTT en IoT”, en Actas del 15º Taller ACM sobre bancos de pruebas de redes inalámbricas, Evaluación experimental y caracterización, 2021, págs. 69–76.

[7] A. Abdul-Rahman, “El modelo de confianza PGP”, EDI-Forum: Journal of Electronic Commerce, vol. 10, núm. 3, págs. 27-31, 1997.

[8] C. Hedrick, “Protocolo de información de enrutamiento”, Grupo de trabajo de red, RFC 1058, junio de 1988.

[9] E. Onica, P. Felber, H. Mercier y E. Riviere, “Publicación/suscripción para preservar la confidencialidad: una encuesta”, ACM Computing Surveys, vol. 49, núm. 2, págs. 27:1–27:43, 2016.

[10] LIW Pesonen, DM Eyers y J. Bacon, “Control de acceso en sistemas descentralizados de publicación/suscripción”, Journal of Networks, vol. 2, núm. 2, págs. 57–67, 2007.

[11] K. Spielvogel, HC Pohls y J. Posegga, “TLS más allá del corredor: aplicación de seguridad y confianza detalladas en entornos de publicación/suscripción para IoT”, en Actas del 17º Taller internacional sobre seguridad y confianza. Gestión, vol. 13075, 2021, págs. 145-162.

3Eclipse Mosquitto: https://mosquitto.org/