MQTT یک پروتکل پیام‌رسان سبک و کم‌مصرف است که برای ارتباطات دستگاه‌های اینترنت اشیاء (IoT) طراحی شده است. این پروتکل به‌ویژه در محیط‌هایی با پهنای باند محدود، تأخیر بالا، یا شرایط شبکه‌ای غیرقابل اعتماد بسیار مناسب است.

۱. تعریف

MQTT یک پروتکل پیام‌رسانی مبتنی بر publish/subscribe است که معمولاً در ارتباطات دستگاه‌ها یا سرویس‌های مختلف که نیاز به ارسال پیام‌های کوتاه و سریع دارند، استفاده می‌شود. در این پروتکل، پیام‌ها از طریق یک سرویس میانه (Broker) به مشترکین (Subscribers) ارسال می‌شوند.

۲. مفاهیم کلیدی

Broker (بروکر): سروری است که وظیفه دریافت، ذخیره، و توزیع پیام‌ها به مشترکین مرتبط را دارد. تمامی دستگاه‌ها به بروکر متصل می‌شوند.

Publisher: این دستگاه‌ها پیام‌هایی را در موضوعات خاص منتشر می‌کنند.

Subscriber (مشترک): دستگاهی است که به‌صورت فعال پیام‌هایی را در موضوعات خاص دریافت می‌کند.

Topic (موضوع): مشترکین می‌توانند به موضوعات خاصی گوش دهند و تنها پیام‌هایی را دریافت کنند که به آن موضوعات مربوط می‌شود.

Message (پیام): داده‌ای که از طرف publisher ارسال شده و در موضوعات مشخص به اشتراک گذاشته می‌شود.

۳. عملکرد

۱ـ۳ اتصال به بروکر

هر کلاینت MQTT برای شروع ارتباط، ابتدا باید به بروکر متصل شود. این اتصال با ارسال بسته `CONNECT` به بروکر صورت می‌گیرد.

داده‌هایی که در بسته `CONNECT` ارسال می‌شود شامل اطلاعاتی مانند شناسه کلاینت، نام کاربری، کلمه عبور (در صورت نیاز) و برخی تنظیمات اختیاری مانند Clean Session و Keep Alive است.

پس از دریافت درخواست اتصال از کلاینت، بروکر با ارسال بسته `CONNACK` به کلاینت جواب می‌دهد. در این بسته، بروکر اعلام می‌کند که آیا اتصال موفق بوده یا خیر. اگر اتصال رد شود، کد خطای مربوطه نیز در این بسته قرار دارد.

۲ـ۳ اشتراک در موضوعات

کلاینت‌ها می‌توانند به موضوعات خاصی که اطلاعاتی را درباره دستگاه‌ها یا وضعیت‌ها نشان می‌دهند، اشتراک کنند. این عمل از طریق ارسال بسته `SUBSCRIBE` انجام می‌شود.

موضوعات درMQTT ، داده‌ها به صورت پیغام‌هایی با یک موضوع خاص دسته‌بندی می‌شوند. هر موضوع ممکن است شامل اطلاعاتی درباره وضعیت یک دستگاه، وضعیت سیستمی، دما، رطوبت، و غیره باشد. موضوعات ساختار سلسله‌مراتبی دارند و ساختار آنها شبیه ساختار URL است. (مانند `/home/livingroom/temperature`)

بسته SUBSCRIBE به بروکر ارسال می‌شود تا کلاینت مشخص کند که می‌خواهد در چه موضوعاتی اشتراک کند. کلاینت همچنین می‌تواند سطح Quality of Service (QoS) را برای هر اشتراک مشخص کند.

۳ـ۳ انتشار پیام‌ها

زمانی که یک کلاینت بخواهد داده‌ای را ارسال کند، بسته PUBLISH را به بروکر ارسال می‌کند. در این بسته، پیام‌ها در یک موضوع مشخص قرار می‌گیرند و به دیگر کلاینت‌های اشتراکی که به آن موضوع گوش می‌دهند، ارسال می‌شود.

بسته PUBLISH شامل داده‌هایی است که قرار است ارسال شوند، همراه با نام موضوع و اطلاعات QoS.

۳ـ۴ انتقال پیام‌ها به مشترکین

بروکر پیام‌های منتشر شده توسط کلاینت‌ها را دریافت می‌کند و آن‌ها را به تمام کلاینت‌هایی که به موضوع‌های مربوطه اشتراک کرده‌اند، ارسال می‌کند.

۳ـ۵ تایید دریافت پیام

MQTT از مکانیزم‌های تایید دریافت پیام برای اطمینان از ارسال صحیح و مطمئن پیام‌ها استفاده می‌کند. این تاییدها بسته به سطح QoS متفاوت هستند. در بخش‌های بعدی سطح‌های مختلف QoS را بررسی خواهیم کرد.

۳ـ۶ حفظ ارتباط

MQTT از یک ویژگی به نام Keep-Alive برای حفظ ارتباط پایدار بین کلاینت‌ها و بروکر استفاده می‌کند. این ویژگی به کلاینت و بروکر اجازه می‌دهد که ارتباط را برای مدت زمان مشخصی حفظ کنند. برای این کار Keep-Alive Interval تعریف می‌شود. این بازه، مدت زمان بین پیام‌های پینگ که برای بررسی وضعیت ارتباط ارسال می‌شود را تعیین می‌کند. اگر بروکر یا کلاینت در این مدت زمانی پینگ نکند، ارتباط قطع می‌شود و بازیابی صورت می‌گیرد.

۳ـ۷ Pingها و پایداری ارتباط

برای اطمینان از زنده بودن ارتباط، از بسته‌های PINGREQ و PINGRESP استفاده می‌شود. این بسته‌ها به‌طور دوره‌ای بین کلاینت و بروکر ارسال می‌شوند تا از قطع نشدن ارتباط اطمینان حاصل شود.

بسته PINGREQ از طرف کلاینت به بروکر ارسال می‌شود تا از وضعیت سلامت و فعال بودن اتصال مطمئن شود. بسته PINGRESP از طرف بروکر به کلاینت ارسال می‌شود تا نشان دهد که ارتباط همچنان برقرار است.

۴. ساختار بسته‌ها

یک بسته MQTT از چندین بخش تشکیل می‌شود که شامل هدر و Payload می‌شود. بسته‌های MQTT معمولاً از سه بخش تشکیل می‌شوند:

۱- Fixed Header: این بخش شامل اطلاعات کنترل بسته است.
۲- Variable Header: این بخش اختیاری است و به نوع بسته مربوط می‌شود.
۳- Payload: داده‌ای که قرار است ارسال شود، مانند پیام یا اطلاعات از دستگاه.

۱ـ۴ انواع بسته‌ها

- `CONNECT`: درخواست برای اتصال به بروکر.
- `CONNACK`: پاسخ به درخواست اتصال.
- `PUBLISH`: ارسال پیام.
- `PUBACK`: تایید دریافت پیام (برای QoS 1)
- `PUBREC`: پیام برای شروع فرآیند تایید دریافت. (برای QoS 2)
- `PUBREL`: تایید دریافت پیام در مرحله بعدی. (برای QoS 2)
- `PUBCOMP`: تکمیل فرآیند تایید دریافت پیام. (برای QoS 2)
- `SUBSCRIBE`: درخواست برای اشتراک در یک یا چند موضوع.
- `SUBACK`: تایید اشتراک در موضوعات.
- `UNSUBSCRIBE`: درخواست برای لغو اشتراک از موضوعات.
- `UNSUBACK`: تایید لغو اشتراک از موضوعات.
- `PINGREQ`: درخواست برای حفظ ارتباط زنده.
- `PINGRESP`: پاسخ به درخواست پینگ.
- `DISCONNECT`: قطع ارتباط.

۵. تشخیص، تصحیح و بازیابی خطا

۱ـ۵ error handling در سطح بسته‌ها

اگر خطایی در اتصال رخ دهد، وضعیت خطا در فیلد Return Code در بسته CONNACK قرار می‌گیرد. این کدها شامل موارد زیر هستند:

- `0x00`: اتصال موفق.
- `0x01`: اتصال رد شد به دلیل نام‌کاربری یا کلمه عبور اشتباه.
- `0x02`: اتصال رد شد به دلیل عدم اجازه.
- `0x04`: اتصال رد شد به دلیل خطا در پروتکل.
- `0x05`: اتصال رد شد به دلیل خطا در ارتباط.

۵ـ۲ QoS و بازیابی خطا

QoS 0: در این سطح، پیام فقط یکبار ارسال می‌شود و هیچ تضمینی برای دریافت آن وجود ندارد. اگر پیام در ارسال یا دریافت از دست برود، هیچ فرآیند بازیابی انجام نمی‌شود.

QoS 1: پیام‌ها حداقل یکبار ارسال می‌شوند. در صورتی که پیام از طرف گیرنده دریافت نشود، ارسال مجدد انجام می‌شود تا زمانی که دریافت آن تایید شود. در این سطح، پیام‌ها می‌توانند دوباره ارسال شوند تا مطمئن شویم که پیام ارسال شده است.

QoS 2: در این سطح، برای ارسال پیام یک فرآیند پیچیده‌تر چهارمرحله‌ای بین فرستنده و گیرنده انجام می‌شود تا تضمین شود که پیام تنها یکبار ارسال و دریافت شود. در صورتی که یک بسته در این فرآیند گم شود، بازیابی به‌صورت خودکار انجام می‌شود.

۵ـ۳ بازیابی ارتباط

در صورت از دست رفتن اتصال، کلاینت‌ها می‌توانند از فرآیند Reconnection برای بازیابی ارتباط استفاده کنند.

مراحل بازیابی اتصال:

۱. در صورت از دست رفتن ارتباط، کلاینت به‌طور مکرر تلاش می‌کند که دوباره به بروکر متصل شود.

۲. بعد از اتصال مجدد، اگر پیام‌های از دست رفته در Queue وجود داشته باشد، کلاینت با استفاده از QoS مناسب، آن‌ها را دوباره ارسال می‌کند.

۳. اگر اتصال قطع‌شده باعث از دست رفتن پیام‌ها شود، بسته‌های تایید برای پیام‌های معلق ارسال می‌شوند.

۵ـ۴ بسته‌های Retained و LWT

Retained Messages پیام‌هایی هستند که بروکر آن‌ها را ذخیره کرده و به هر مشترک جدیدی که به یک موضوع خاص اشتراک می‌کند، ارسال می‌کند.

LWT به‌صورت پیش‌فرض و به‌طور اتوماتیک توسط کلاینت‌ها تنظیم می‌شود تا در زمانی که ارتباط قطع شد، پیام خاصی از طرف آن‌ها ارسال شود. این پیام می‌تواند به دیگر کلاینت‌ها اطلاع دهد که دستگاه یا کلاینت موردنظر از دست رفته است.

۶. ترافیک و کنترل جریان

MQTT به‌طور ضمنی برای جلوگیری از ازدحام ترافیک طراحی شده است. همانطور که گفته شد بسته‌ها به صورت ساختار سلسه‌مراتبی دسته‌بندی می‌شوند و کلاینت‌ها تنها به موضوعاتی که اشتراک دارند گوش می‌دهند. این ساختار باعث می‌شود که هیچ ترافیک غیرضروری به دستگاه‌ها ارسال نشود.

۷. امنیت

اگرچه MQTT خود به‌طور پیش‌فرض مکانیسم‌های امنیتی خاصی ندارد، اما می‌توان از روش‌های زیر برای افزایش امنیت ارتباطات استفاده کرد:

- TLS/SSL برای رمزگذاری ارتباطات.
- احراز هویت با استفاده از نام کاربری و کلمه عبور.
- Access Control برای محدود کردن دسترسی به موضوعات خاص.