January 08, 2018

Intelligent routing methodology for IOT

Grace Priscilla Nambi
Hewlett Packard Enterprise

Intelligent routing methodology for IOT

Abstract

There is a rapid shift to the internet of things in the fast moving world of technology and there could be billions of heterogeneous entities communicating to one another within a span of 10 years. The IOT market is still evolving initiating changes that is triggering growth in various aspects for virtualization and cloud computing. In spite of all the progress made thus far, it is tough to get into the various operational fields and complexity involved in multiple divergent areas of intercommunication.
The purpose of action involving these field also vary. In this situation it will become hard to segregate and speed up communication among various entities based on priority and purpose, opening up a way for the need of a unique specifier or identifier that conveys facts about the purpose of an entity added in the IOT network based on which the message can be routed.

Problem statement

IOT is increasing rapidly today and there are difficulties as we have multiple entities associated with the IOT network varying from banking transactions to a small vendor transaction, varying from signaling notification for an emergency to a common friendly chat and from location identification to a simple validation of the existence of a particular device of importance. The supported communication standards vary for different entities. Some could be using WiFi, some on LTE, some could be using CDMA, some on cloud computing and so on. There isn't any way to segregate and distinguish the IOT traffic messages coming from different service entities or the purpose of the different message sent by the same entity. There also isn't any methodology available to pick the right choice and drop unwanted messages during congestion state.

Solution

This solution proposes an "identity-based" framework with "purpose-based" or "service-based" routing model based on priority for which the choice of a device relies on the identity of the thing/object linked with its purpose. Whenever an object/things gets associated with the IOT network, the identity of the object is constructed by the router from the security, end-to-end communication protocols (could be MQTT, XMPP, CoAP etc), the application purpose etc. The extracted identity contains information on the purpose (message type), supported protocols and the device. The identity then gets inserted as a middleware layer named IOT identifier in-between the application and the data communication layer.

Every entity that requires to route information in the IOT network should thus possess a self-identifier which carry the purpose, urgency, security, protocol, application type and acknowledgement requirement. Whenever a router receives a message it first extracts the IOT Identifier layer from the message.

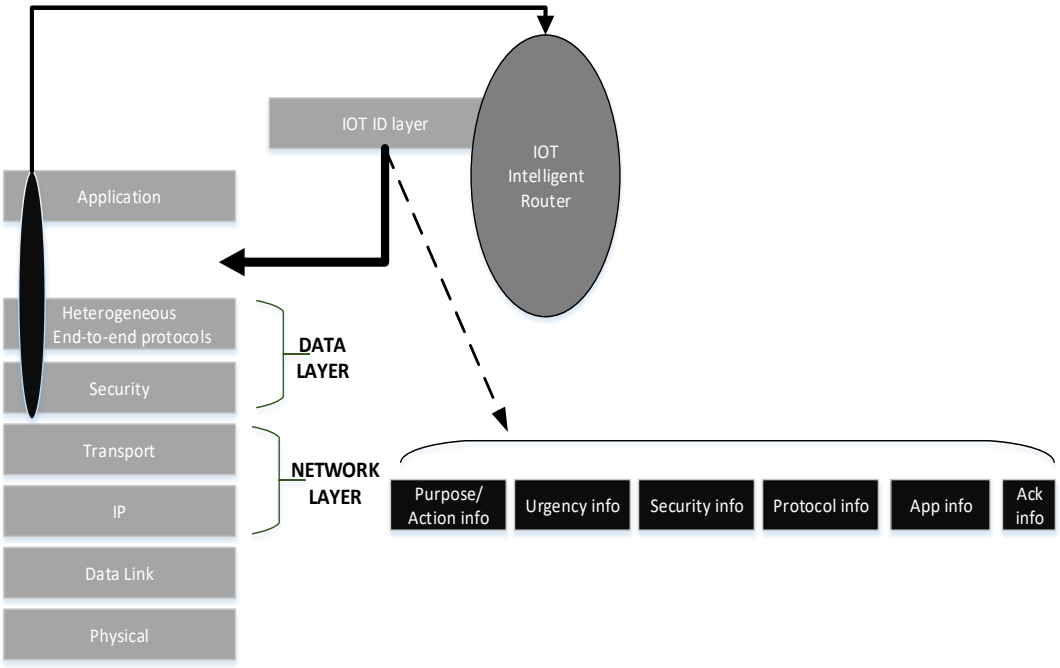

Figure: 1 Architecture

Every router can visualize a tree of information just based on the identity of the thing/object which is the purpose it is going to serve. It is fetched from application later in addition to details on the lower layer protocols (communication and security). The purpose is to be clubbed with the action. The action for every identifier is available to the router from the identifier.

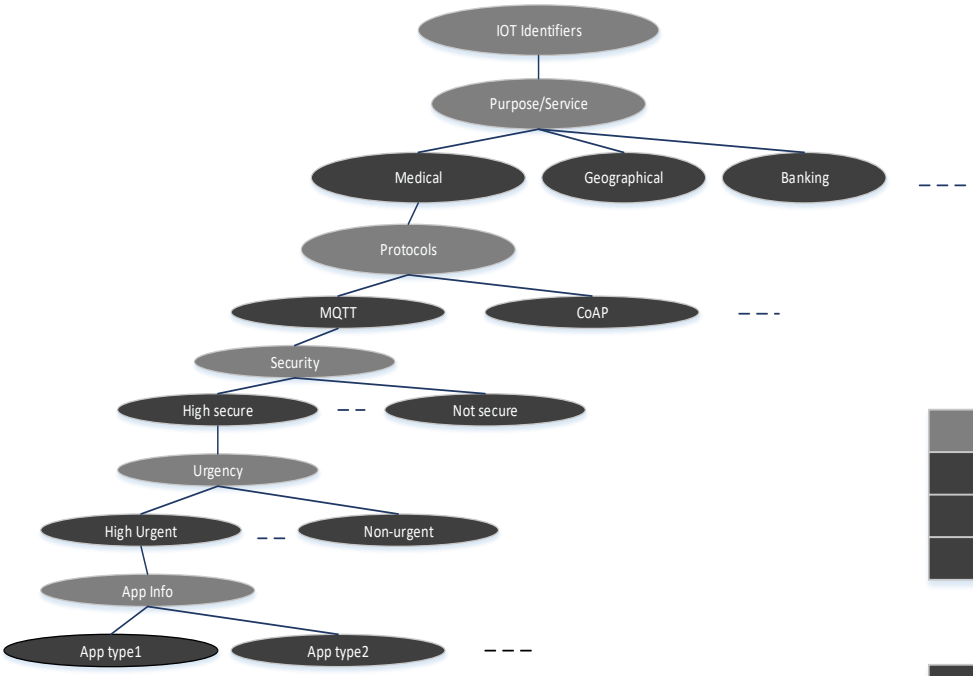

Figure: 2 Device-info organization

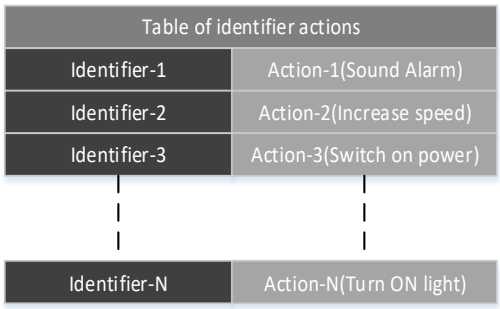

Figure: 3 ID-action info

A sample of the extracted message from the identifier could be of the below type.

{Purpose info:Medical|Urgency info:critical|Security info:Low|Protocol info:CoAP|App info:Device+Action|Ack info}

If the IOT network agreed code for these entities are {1000|0100|0001|0100|0110+10101+0} - this becomes the identifier. If the Ack info is “0” it means no response is required for the sender in this case.

There is an initial handshake for registration of any IOT device to the IOT network followed by the message type’s exchange - of the desired action on the device. This is a onetime handshake having “IOT register req” and IOT register res” message types wherein the device gets its identity. Following which the router of the device joining with the network gets the information of all the identities updated which has the action embedded in the identities for all the entities. When any action is triggered the “IOT action req” message is sent to its router which searches the identifier responsible for the particular action triggered. The logic in the router will first

- Sort all the identifier with same action
- Choose from the identifier list the right device which ensures no re-trials or unwanted messages delivery that can congest the network.
- The right device means, it is the one that has the required action, right urgency, secure if required for that specific action and matching communication IOT protocols.
- In case if something does not match the best is considered and the receiver router takes care of the rest.

When a router receives an IOT message it extracts the middleware IOT identifier layer. From the sender identifier, it checks the compatibility. In case, there is a mismatch in the communication IOT protocols, it makes decision to send it to the protocol convertor before triggering the device for the action.
After the action is triggered it sends back the response sending “IOT-R action res” message stating whether action is accomplished or unaccomplished. Again, the response is “optional” based on the sender identifier acknowledgement info.

Illustration:
Making use of the above methodology we have a real use case for which this methodology solves the problem quickly and accurately.

Consider a future smart city comprising of multiple smart devices connected over IOT network. Each of which has a different purpose to serve. A smart vehicle allocator receives a message from 3 different entities for which the router associated which the smart device extracts the identifier from the middleware layer.
Identifier 1 is {0110|0100|0001|0101|0111+10101+0}
Identifier 2 is {0011|0000|0001|0110|0111+10101+0}
Identifier 3 is {1111|1111|0001|1100|1101+10101+1}
(The above provided set bits are agreed upon standard for this IOT network). The same for all the three which could be to trigger action of sending a vehicle to the source spot.
The first message is from an “office book vehicle” app triggered from a smart device (could be an office bag taken up to get ready to go to office). The purpose here is “go to office”. The second message is from a tourist triggered from his “book tourist visit” app from a smart device (could be his mobile itself). The purpose here is to “go to tourist spot”. The third message is from accident alarm device. The purpose here is “go to hospital”.

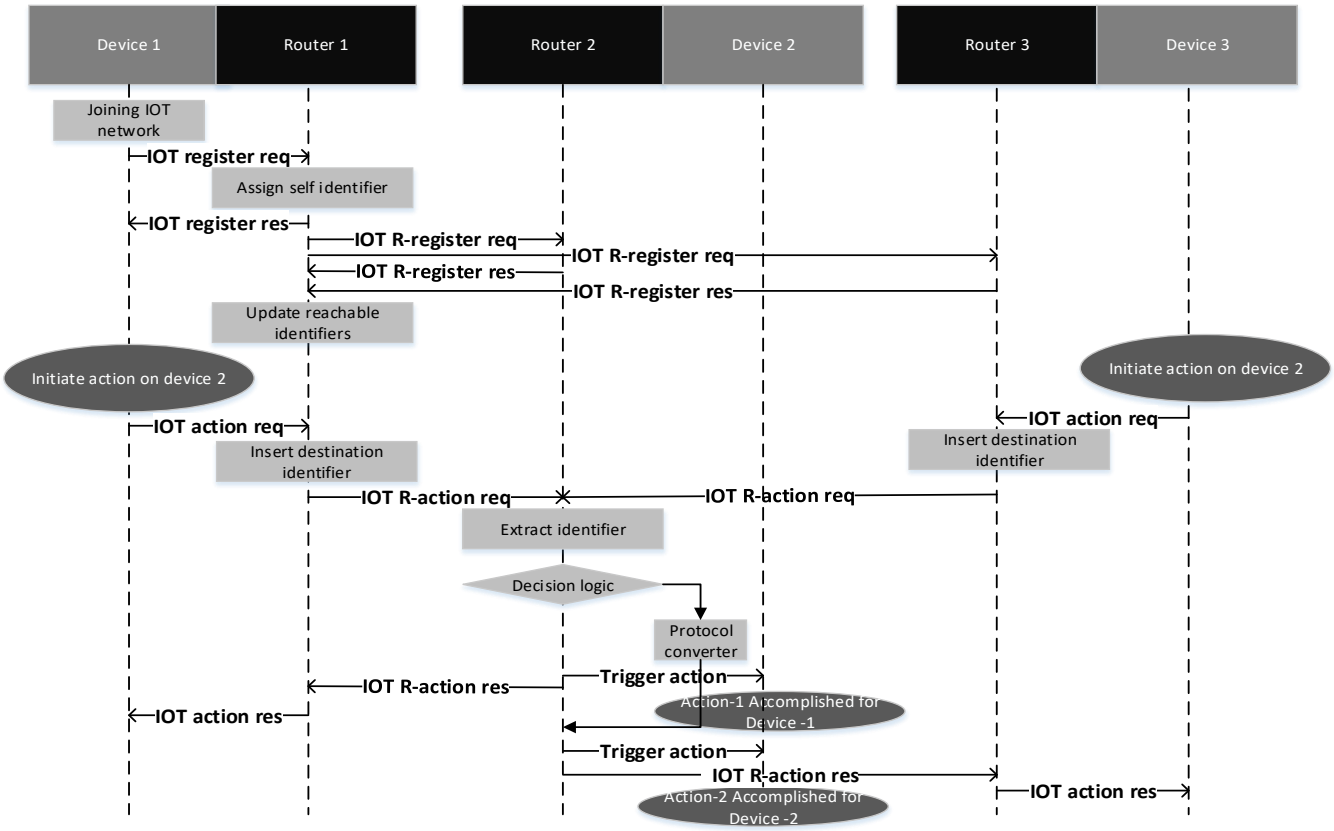

Figure: 4 Call Flow

The router has the business logic to identify the purpose/urgency/security level/supported protocol/app info+action/Ack requirement. It can easily prefer to do the action for identifier 3(medical need of high priority). It also ensures to send the acknowledgement once action is triggered. Also during high traffic it can choose to drop the message from identifier 2 which is of “0000” priority or urgency. The business logic also ensures conversion in a protocol inconsistency case.

There can also be a business logic to process only medical services. In that case if his identifier is “1111” for medical info the sender router will not route unnecessary messages to him reducing the network congestion. His choice is well conveyed at initial registration itself. It thus has reduced application overhead.

How is the solution unique?

There are event based routing approaches available that operates based on the context. In such cases, a device subscribes to an action and every subscriber is notified on the occurrence of that action. This will result in unnecessary messages being exchanged in the IOT network and cause congestion.

- It is a purpose driven approach
- All details of identity is revealed at start up
- Reduces congestion

Conclusion

This approach is being explored for providing a better routing technology for the rapid growing internet of things.

Grace Priscilla Nambi, Hewlett Packard Enterprise