Relatório - Redes Mesh, a alternativa à rede tradicional

Departamento de Engenharia Informática e de Sistemas (DEIS)

Bruno Alexandre Ferreira Pinto Teixeira (a2019100036)

18-04-2021

Conteúdo

Lista de figuras

1 Introdução

Este trabalho tem como objetivo explicar o conceito de Rede Mesh e o funcionamento da mesma numa perspetiva técnica.
Visa tambem falar sobre IoT em Redes Mesh e as suas vantagens e desvantagens assim como segurança em Redes Mesh.
É dado algum ênfase à parte da segurança uma vez que é algo importante e indespensável de conhecimento.

2 Desenvolvimento

2.1 Rede Mesh

A rede mesh é uma topologia de rede local em que os nós/modulos existentes na mesma estão ligados entre si diretamente de uma forma dinâmica e não hierarquica. Este tipo de tecnologia permite criar um sistema Wi-Fi formado por pelo menos dois dispositivos, criando assim uma rede única.
Esta organização cria uma independência entre os nós, fazendo com que cada nó participe na distribuição de informação, para os clientes, de maneira única e bastante eficiente.

O própio nome **mesh** remete para uma **malha**, malha esta que é criada quando todos os nós estão conectados uns aos outros cobrindo assim toda a infraestrutura, conseguindo distribuir um sinal Wi-Fi.

2.1.1 Funcionamento de uma Rede Mesh

As redes mesh utilizam duas tecnicas bastante conhecidas para transmitir informação para os vários nós, uma delas chamada de ***flooding*** e outra de ***routing***.

Flooding refere-se a um algoritmo de *routing* em que cada pacote de rede é enviado para todos os próximos nós, tornando-se assim um algoritmo confiável uma vez que mesmo havendo perca de pacotes a meio, um nó recebe na mesma a informação por outro caminho alternativo.
No entanto isto leva a um aumento do congestionamento da rede, contudo a integridade da informação é quase sempre garantida.

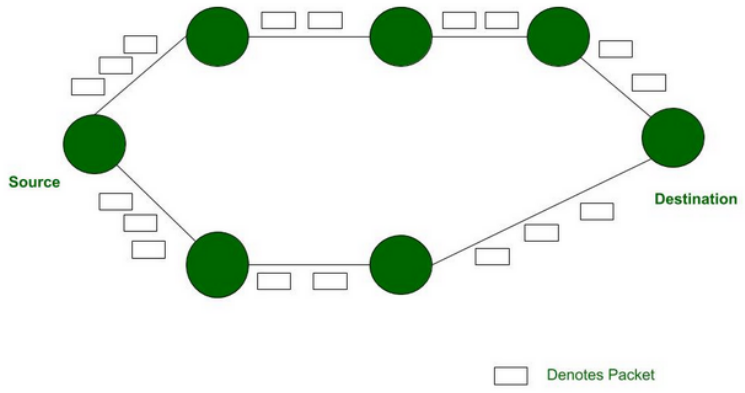

Figura 1: Flooding

No *routing* em vez de ser enviado o pacote de rede cegamente para todos os caminhos possíveis, é definido um caminho de destino, fazendo com que o pacote dê "saltos" de nó em nó até chegar ao destino final.
Para que todos os caminhos estejam disponíveis no caso de um caminho "partido", a rede garante uma conexão contínua usando algoritmos de auto recuperação, algoritmos estes que encontram alternativas de encaminhamento em caso de desastre. Neste caso a rede não fica tão congestionada uma vez que estamos a usar apenas um caminho necessário para chegar ao destino final.

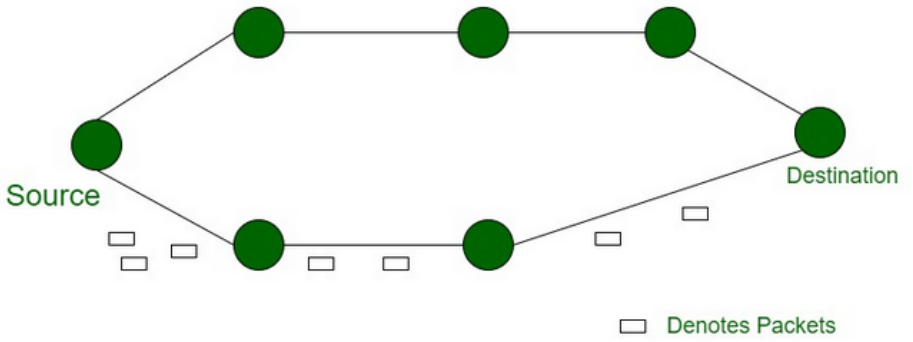

Figura 2: Routing

A estrutura destas redes é constituída por um nó com o intuito do mesmo ser o router principal da rede mesh. Este router está diretamente ligado ao router do **ISP** que garante o acesso à **Internet**.
Depois temos vários nós que irão estar ligados ao router principal, ramificando para outros, em que podemos ter todos os nós ligados entre si ou então só alguns ligados entre si, fazendo assim a distinção entre uma rede mesh parcialmente conectada ou uma rede mesh totalmente conectada.

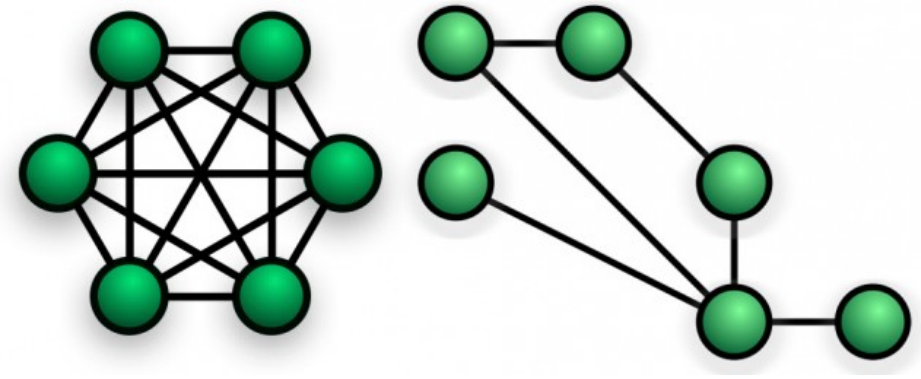

Figura 3: Diferentes arquiteturas da rede mesh

2.1.2 Como instalar uma rede mesh

Antes de instalar uma rede mesh é preciso ter em consideração várias coisas, uma delas é por exemplo o espaço total até onde pretendemos ter acesso à rede para podermos ter uma noção do número de equipamentos que precisamos de adquirir. Para o nó principal é preciso arranjar a localização ideal para que seja possível conectá-lo a varios nós. Normalmente a melhor zona fica situada no meio da casa mas longe de zonas de obstrução.
Depois é preciso perceber qual será a melhor localização para os nós seguintes. Habitualmente estes são ligados a tomadas e ficam longe de fontes de interferência como por exemplo microondas, telefones sem fios, etc.

Depois de escolhido o sítio para os equipamentos, já é possivel instalar uma rede mesh. Existem vários sistemas mesh e geralmente todos estes usam uma *app* para controlar o sistema.
O passo seguinte é ligar um nó (nó principal) ao router **ISP** e de seguida ligar o router a uma tomada. Ao ligar o router , a *app* vai detetar que o router está ligado e vai pedir para ser criada uma conta e logo de seguida pede para que seja feito um *scan* do ***QR code*** para *linkar* o nó principal à *app*.
No fim, pede uma estimativa de nós a serem utilizados na rede, número que pode ser alterado sem problemas sempre que se acrescenta ou se retira um nó à rede, e pede que o utilizador confirme se em cada nó conectado existe conexão à internet e à rede interna.

2.1.3 Vantagens e Desvantagens

Como em todo tipo de topologia existem vantagens e desvantagens, no entanto neste caso as vantagens destacam-se comparativamente às desvantagens.

Uma das principais vantagens é o facto da sua instalação ser extremamente simples, assim como o seu processo de manutenção.
A *app* é um benifício enorme uma vez que permite ver toda a especificação da rede, desde velocidades, qualidade de conexão entre nós, qualidade física dos nós, controlo parental,etc.
É extraordinariamente adaptável e flexível fazendo com que no futuro seja possível aumentar o seu alcance conectando novos nós sem ser preciso qualquer tipo de configuração, tendo por base o princípio de ***plug and play***.

Uma enorme desvantagem é o facto de que para se construir uma rede mesh é preciso que seja feito um investimento grande devido ao seu elevado custo relativamente ao hardware necessário.

Em Portugal, um sistema mesh custa em média 200 euros o que faz com que não seja um sistema tão habitual comparativamente com a rede tradicional.

2.2 IoT em Redes Mesh

Uma rede IoT (Internet of Things) consiste em vários sistemas embebidos que podem controlar sensores de temperatura, válvulas de água, etc.
Todos estes sistemas precisam de estar ligados à Internet para poderem ser controlados remotamente. Para que isto aconteça, precisamos de garantir que estes sistemas estão protegidos, uma vez que estão expostos, e que estejam sempre disponiveis.

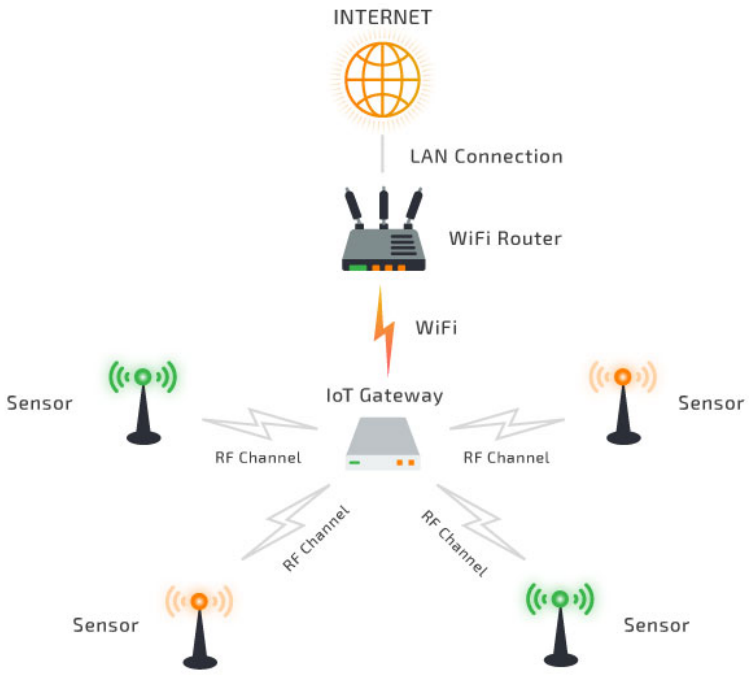

Figura 4: Topologia tradicional de uma rede IoT

Esta topologia tradicional funciona bem até um certo ponto. Quanto mais sensores existirem pior ficará o *IoT Gateway* uma vez que o mesmo tem um limite fixo de sensores que consegue suportar. Outro problema é quando temos vários sensores que partilham a mesma frequência no mesmo sitio provocando colisões na comunicação.

Usando uma topologia *Mesh IoT* continua a ser preciso um *IoT Gateway* no entanto o mesmo apenas está ligado a alguns sensores e não a todos os sensores presentes na rede, facilitando assim o processo de comunicação e evitando a sobrecarga de sensores no *IoT Gateway*.

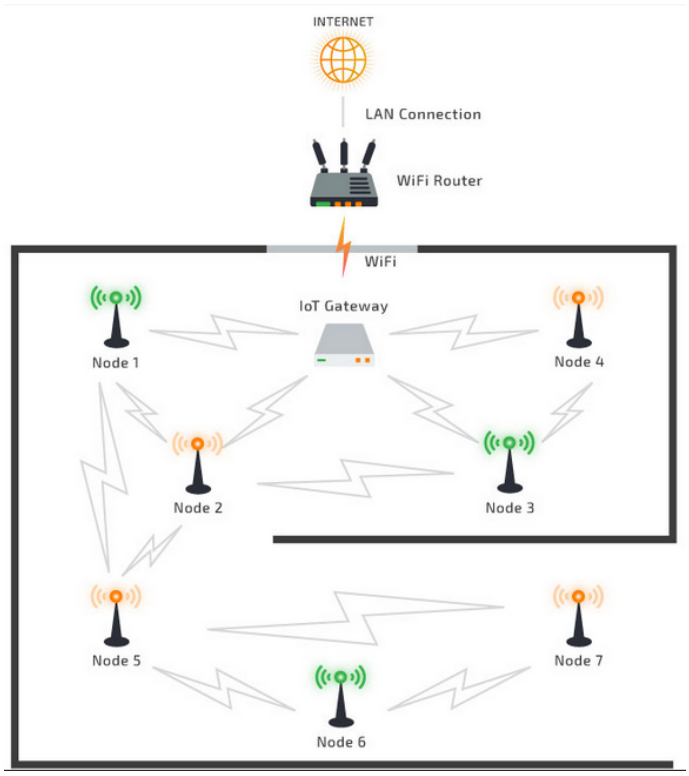

Figura 5: Topologia Mesh IoT

2.3 Segurança em Redes Mesh

Atualmente a segurança é bastante importante uma vez que todos os dias há novos ataques aparecer. Por isso é importante que a nossa rede (mesmo sendo uma rede doméstica) esteja segura.
Uma vez que existem diversos protocolos usados nas Redes Mesh, temos de estar atentos a falhas de segurança nos protocolos pois estes são responsáveis pela maior parte do *workflow* da rede.
Por defeito os protocolos de *routing* assim como os protocolos da subcamada *medium access control (MAC)* assumem que os nós não têm más intenções, por isso concluem que podem confiar nos mesmos para usarem o protocolo *MAC* e para ser feito o *routing*.
Como existe este conceito de **confiança** entre nós, o nó vizinho nunca verifica se a informação recebida é ou não legitima, criando aqui um grave problema.

Por exemplo, um **nó malicioso** pode enviar para outro nó vizinho, informação manipulada na tabela de *routing*, informação que não é verdadeira e pode comprometer a rede. O mesmo **nó malicioso** pode tambem não enviar pacotes de dados, fazendo uma espécie de barreira ou ao contrário, pode enviar demasiados pacotes

de dados originando assim um possível ataque de **DoS** *(Denial of Service)*.

2.3.1 Ataques na camada física

Todas as redes *wireless* são vulneráveis a ataques de *radio jamming* na camada física.
Este ataque é bastante grave uma vez que bem executado pode levar a que a rede vítima deixe de receber o sinal necessário à comunicação.
É um ataque fácil de ser implementado pois só é preciso que um dispositivo *wireless* transmita um sinal forte o suficiente para bloquear o processo de comunicação.
Existem vários subtipos de ataques *radio jamming*, por exemplo, *constant jammer* em que o atacante envia continuamente um sinal bloqueando a comunicação, *reactive jammer* em que o atacante só envia um sinal quando existe comunicação na rede vitima.

2.3.2 Ataques na subcamada MAC

Nesta subcamada existem alguns ataques como por exemplo, *passive eavesdropping*, *MAC Spoofing*, etc.

Dado que neste tipo de rede os pacotes de dados são transmitidos usando "saltos" de nó em nó, esta está sujeita a um ataque de *passive eavesdropping* pois um **nó malicioso** pode guardar a informação que está a ser transmitida na rede. Neste caso a *performance* da rede não é afetada mas pode haver informação confidencial a ser extraída sem permissão.

Atualmente é bastante simples disfarçar ou alterar o endereço MAC de um dispositivo e é nisso em que consiste o ataque *MAC Spoofing*. Isto faz com que possamos disfarçar o nosso **nó malicioso** com um endereço MAC legítimo. Os administradores de redes costumam guardar os endereços MAC verídicos numa lista de acesso, fazendo com que só aqueles endereços possam se conectar a um certo nó, mesmo assim é possível ganhar privilégios na rede usando um endereço MAC autorizado.

Os ataques descritos anteriormente só são possíveis estando fisicamente na rede vítima.

3 Conclusão

Como foi visto anteriormente, as Redes Mesh são uma mais valia para serem usadas em alternativa a uma simples rede tradicional.
O custo monetário ainda é um bocado elevado, no entanto a qualidade e fiabilidade da rede é muito superior comparando com a rede tradicional usada.

Estas redes já comprovaram a sua eficiência, por exemplo no terramoto do Haiti, o projeto Australiano *Serval* foi criado para fornecer comunicações de emergência enquanto a rede telefónica e as redes Wi-fi estavam inoperacionais.
O projeto tinha uma aplicação que permitia as pessoas comunicarem entre si, usando Wi-Fi, até uma distância de 100 metros.

4 Bibliografia

- https://en.wikipedia.org/wiki/Mesh_networking
- https://en.wikipedia.org/wiki/Flooding_(computer_networking)
- https://en.wikipedia.org/wiki/Routing
- https://www.quora.com/
- Security in Wireless Mesh Networks by Yan Zhang, Jun Zheng and Honglin Hu
- https://paulhugel.wordpress.com/2010/10/18/the-serval-project/