Providing quality of service in wireless ad hoc networks

Catharina Candolin*
Catharina.Candolin@hut.fi

Maarit Hietalahti*
Maarit.Hietalahti@hut.fi

Hannu H. Kari*
Hannu.Kari@hut.fi

*Laboratory for Theoretical Computer Science
Helsinki University of Technology
P.B. 5400, FIN-02015 HUT, Finland

Abstract

This paper presents a combined security and quality of service model for wireless ad hoc networks. The model is based on the fact that quality of service cannot be guaranteed unless the sender of the packets is authenticated. Authentication takes place both on node-to-node level and access level. Once the node is authenticated, it can be granted a given level of quality of service. Quality of service is transitively provided, which means that an access point can sell part of its capacity to neighboring nodes, which in turn can sell part of their capacity further as long as the agreed limits are not exceeded. This scheme significantly simplifies the quality of service provisioning in wireless and wired networks.

1 Introduction

Providing guaranteed quality of service to a mobile node in a wireless network is a difficult task. In commercial wireless networks, quality of service is often bundled together with the access control and payment services. For example, in telecommunication networks, a significant part of the complexity comes from the effort to ensure the promised quality of service to each mobile node.

Payment for the access service is not an issue in a military environment, but providing quality of service is as crucial as in commercial networks. Sharing and controlling the usage of resources is important in order to ensure that low priority data does not prevent high priority data from being delivered. Furthermore, the network needs to disable malicious nodes from disrupting network communication.

In this paper, we propose a combined security and quality of service model. Our model is based on the fact that quality of service cannot be guaranteed unless the sender of the packets is authenticated. Authentication can be done, for example, by using standard IPsec ESP [3][4] encapsulation.

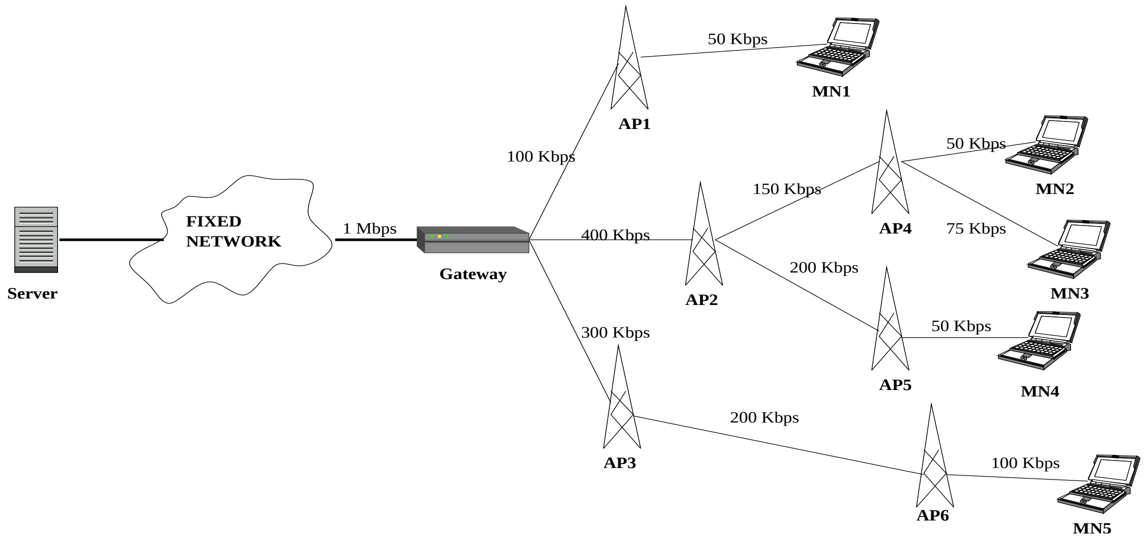

Figure 1: Interconnection of fixed and ad hoc networks

2 Quality of Service

When an ad hoc network is attached to a fixed network via a gateway, the gateway must control the quality of service of all nodes connected to it. A node can be either a Mobile Node (`MN`) or an Access Point (`AP`), which is dedicated to providing MNs access to a fixed network. The gateway (`GW`) is an access point that has a connection both to the fixed network and the wireless ad hoc network. An example of such a network is depicted in Figure 1.

In our model, quality of service is transitively provided at node-to-node level. For example, as in Figure 1, if the gateway has 1 Mbps guaranteed capacity to the fixed network, it may redistribute to its neighboring nodes `AP1`, `AP2`, and `AP3` the capacities of 100 Kbps, 400 Kbps, and 300 Kbps respectively, and keep 200 Kbps for itself. The neighboring nodes can sell their capacities further, for example, `AP1` may sell 50 Kbps to `MN1`, `AP2` may sell 150 Kbps and 200 Kbps to `AP4` and `AP5`, and `AP4` may sell 50 Kbps to `MN2`, and so on. When policing the QoS, it does not matter from where the traffic is originated, as long as its neighbors do not exceed the agreed limits. That is, `AP2` does not care from which MNs the traffic is originated, as long as `AP4` and `AP5` do not send more traffic than they are entitled to. In such a case, the traffic exceeding the limits can be discarded.

3 Security Architecture

In order to provide quality of service, authentication must be performed. In our model, this is done on two different levels, node-to-node and access level. Node-to-node level authentication takes place between the two nodes that participate in routing the packets. Access level authentication is done between the gateway and the mobile node. For example, in Figure 2, node-to-node level authentication is performed between the gateway and `AP2`, between `AP2` and `AP5`, and between `AP5` and `MN4`. Access level authentication is performed between the gateway and `MN4`.

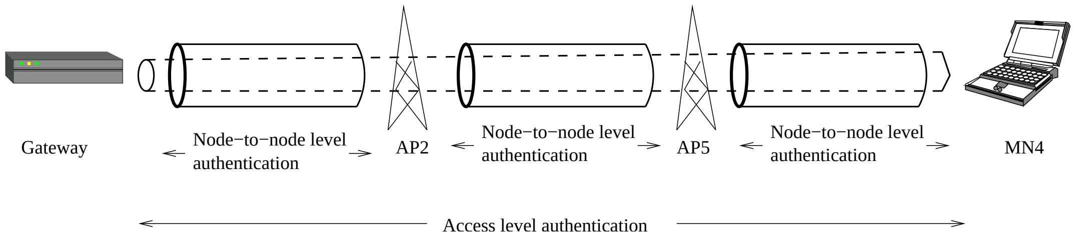

Figure 2: Node-to-node and access level authentication

Node-to-node level authentication is necessary for distinguishing the origin of the data packets, so that the agreed level of quality of service can be provided for the sending node. For example, `MN4` authenticates itself to `AP5`. `AP5` in turn authenticates itself to `AP2`, and so on. The AP is responsible for controlling the usage of network resources by its peers. If any peer consumes more bandwidth than it is allowed to, the AP can choose to drop the exceeding packets, regardless of whether it at that point is able to forward them or not. Node-to-node level authentication is important for two reasons. First, it makes it possible to prioritize packets so that high priority traffic is delivered even if the network load is high. Second, the network is likely to consist of compromised nodes that will try to use the network resources to their advantage. Therefore, controlling the use of resources prevents such nodes from disturbing the network and limits the scope of denial-of-service attacks caused by flooding.

Access level authentication is needed between the gateway and each mobile node in order to control the traffic flow from the fixed network to the ad hoc network. For example, if the server in Figure 1 is malicious and floods a MN, the gateway should be able to drop the packets exceeding the capacity provided to the MN in question. Another possibility would be to perform authentication between the gateway and the server by relying on IPSec, but this would require some kind of trust management and PKI in the fixed network.

3.1 Packet encapsulation using IPsec

Authentication can be done, for example, by using IPsec ESP encapsulation with null encryption. Null encryption is sufficient on this level, since the only security service that is needed is authentication. The IPv6 [1] packet intended for the destination is first encapsulated in another IPv6 packet, which is protected with ESP. This first tunnel is formed between the `MN` and the `GW`, and it provides access level authentication. The encapsulated packet is encapsulated once more in another ESP protected IPv6 packet. This second tunnel provides node-to-node level authentication and is performed between each two nodes respectively. For example, the packet encapsulated by `MN4` is decapsulated at `AP5`, which then encapsulates the packet for `AP2`.

In order to establish such tunnels, the nodes need to have a Security Association (SA) with each other. For example, in Figure 2, an SA needs to be established between the `GW` and `AP2`, between `AP2` and `AP5`, between `AP5` and `MN4`, and between the `GW` and `MN4`. The SA can be established using any key exchange protocol, such

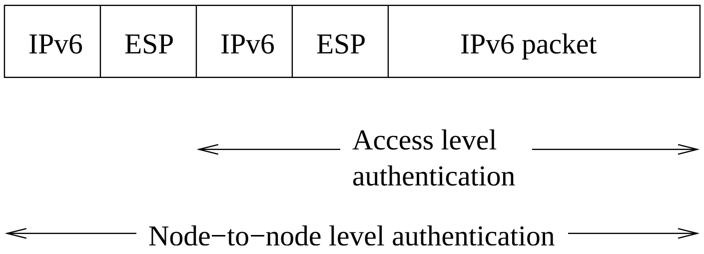

Figure 3: Authentication protocol

as IKE [2].

4 Conclusion

This scheme simplifies the QoS provisioning in wireless and also wired networks, since the controlling of the QoS is distributed in the network, and the nodes can independently sell their capacity further. Thus, each node only needs to know the negotiated QoS of its incoming and outgoing links. The gateway also needs to know the negotiated QoS of each mobile node in order to protect the network from denial-of-service attacks, but it does not need any information about the paths between the APs. For example, as in Figure 1, the gateway knows the negotiated QoS level of its neighbors `AP1`, `AP2`, and `AP3` as well as the negotiated levels for `MN1`, `MN2`, `MN3`, `MN4`, and `MN5`. However, the gateway does not need to know the negotiated QoS between e.g. `AP3` and `AP6`.

QoS can be guaranteed only if the sender of the packets is authenticated. Therefore, in our solution, the nodes are authenticated both on access and node-to-node level. Access level authentication is done between the gateway and the mobile node, whereas node-to-node level authentication is done between all neighboring nodes.

Acknowledgments

This research has been funded by the Finnish Defence Forces.

References

[1] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. Request for Comments 2460, 1998.

[2] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). Request for Comments 2409, 1998.

[3] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). Request for Comments 2406, 1998.

[4] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. Request for Comments 2401, 1998.