**Environment**

Future Internet?

User can connect Internet at anytime and anywhere.

Next Generation all IP communication.

**Problem or issue**

Require secure communication to take place only between a dynamic subset of distributed devices sharing a common context.

**Requirement & Characteristic**

* Membership configuration and management

composition can change over time.

* Distributed Operation

distributed member discovery and VPAN formation and maintenance.

* Security
* Self-organization and mobility management

be able to discover each other and form a secure overlay without user intervention.

* Application support

User should be able to specify which applications, services, data are reachable through or have access to a specific VPAN.

* Local private address space

Each VPAN will have its own local private address space, separated from the global IP address space. why? Applications running within a VPAN use this private address independent of changes in the global address of the node due to node mobility.

* Ad hoc routing and tunnel management

Apart from its own addressing scheme, each VPAN also has its own internal routing mechanism.

* Scalability

The number of members forming the VPAN can become quite large.

Related Works

표 한장으로 표시.

**Proposed Scheme**

Virtual private ad hoc networks(VPAN) are secure and self-organizing overlay networks on top of existing IP infrastructure that use ad hoc networking techniques to enable network connectivity.

Creates a transparent, shielded and trusted environment for the applications and services running on the

participants' devices.

* High-Level Network and Node Architecture
  + High-level Network architecture

1. Localized VPAN

All members are interconnected either wired or wireless without using any non-member nodes.

2. Distributed Intrastructured VPAN

connectivity has to use non-member nodes as relays in order to forward their traffic.

Tunneling needed.

The members are interconnected over the Internet, using nodes in the infrastructure a relay.

Infrastructure support can assist the VPAN membership management, member discovery, formation, routing and mobility management.

Similar with Personal Network concept.

3. Distributed Ad Hoc VPAN

ad hoc nodes are used as relays.

VPAN membership management, member discovery, formation, routing and mobility management has to be done in a completely distributed manner.

4. Hybrid VPANS

Combination of the above architectures.

* + High-level node architecture

어려운 파트다-,- 자세히 보자.

**Challenges**

1. VPAN definition and management
   1. Its policies and its members, or its membership rules, first have to be defined. The creation of a new VPAN will be triggered by a service provider or, more commonly, by an individual person.
      1. Who is the creator of the VPAN?
      2. How and where is the VPAN definition and membership information stored and/or distributed?
      3. When can the VPAN be formed and become operational?
      4. How are new members added to the VPAN(membership policies)?
      5. Member authentication?
   2. One of the members invite or request join to creator.
   3. Define membership rules and automating the process of member addition.
2. Security
   1. Member identification and authentication
   2. Authentication of communication between VAPN members.
   3. Confidentiality of communication between VPAN members.
3. VPAN formation and self-organization
   1. Member discovery mechanisms form the basis of the formation of the VPAN overlay, as it is needed for secure link and tunnel establishment between member nodes.
4. Addressing and routing
   1. Within the overlay, the members will use private IP addresses and will run an ad hoc routing protocol. As such, the overlay is used to transparently exchange VPAN data and control messages, using the public IP infrastructure as carrier.
   2. Each VPAN will have its own local address space, from which each member is assigned one address, independent of its number of interfaces. All applications and services that communicate within the VPAN will use this address. This address space is confined within the VPAN and invisible to the outside world by tunneling or link encryption.
   3. When running multiple VPANs within the same device, their need to be distinguishable => Different VPAN using different address prefix.
5. Member mobility management
   1. Localized VPAN
      1. Member discovery and link break detection mechanisms can improve VPAN maintenance.
   2. Other
      1. Member mobility => change of public IP address => breakdown of tunnels established between members of the VPAN overlay => require dynamic tunnel reestablishment mechanisms and interaction with the membership management or member discovery framework.
6. Application middleware
   1. The main functionality of this component is to act as a firewall for the resources and services at the higher layer.
   2. Be able to specify to what extent their applications and services have access to the VPAN and to what extent other and services need to be able to specify the VPAN they want to use.
   3. A powerful interface between the VPAN protocol stack and the service and application layer is needed
      1. => form of a platform independent generic middleware system.
7. Etc
   1. Naming, QoS, context information to improve networking and management, intrusion detection, dealing with multiple or event hierarchical VPANs, traffic optimization.