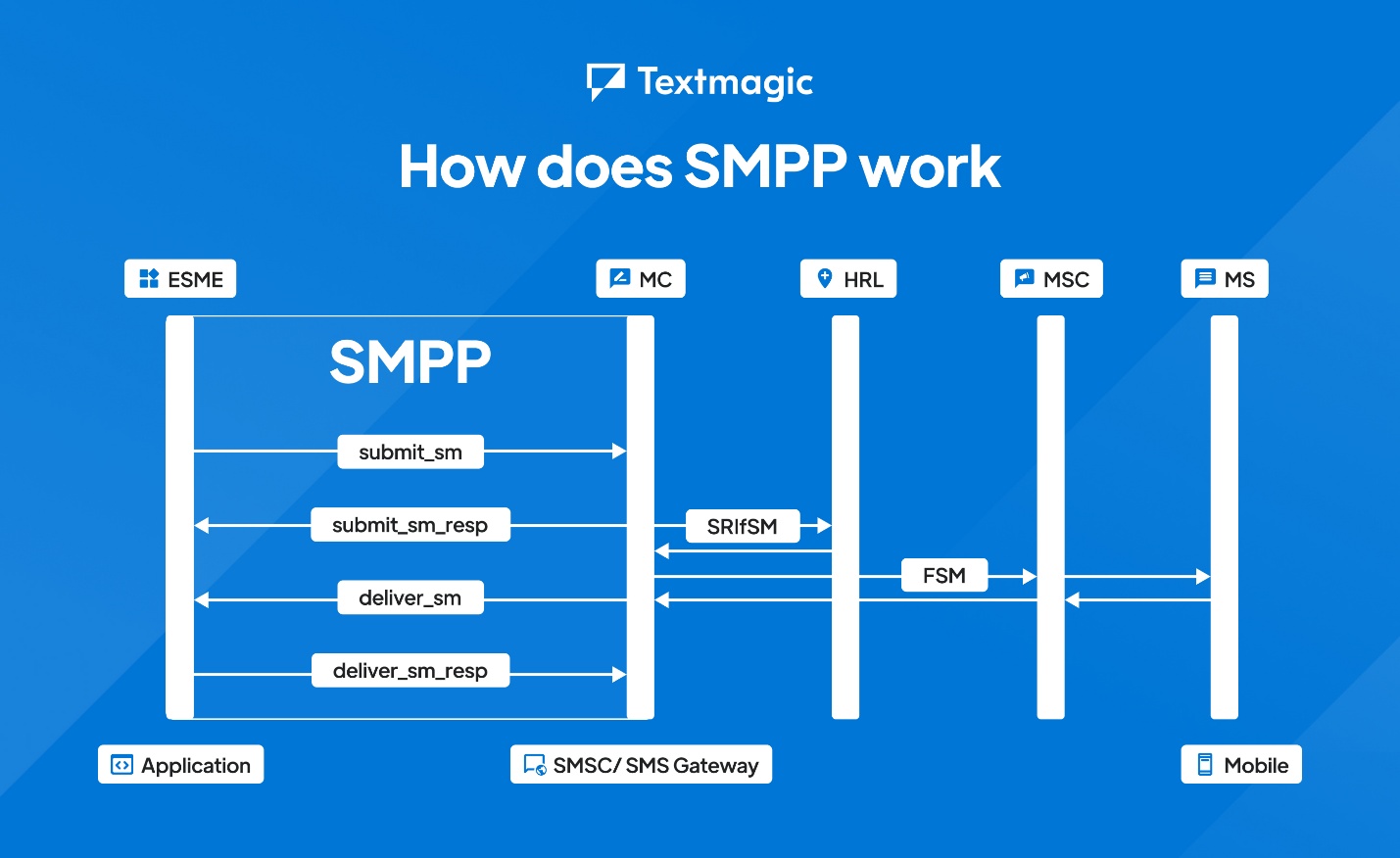
**SMPP**

-Giao thức SMPP (Short Message Peer-to-Peer) là một giao thức mở, chuẩn công nghiệp được thiết kế để cung cấp giao diện truyền dữ liệu linh hoạt cho việc truyền dữ liệu tin nhắn ngắn giữa các Thực thể tin nhắn ngắn bên ngoài (ESME), Thực thể định tuyến (RE) và Trung tâm tin nhắn (MC). Đây là phương tiện mà các ứng dụng (gọi là ESME) có thể gửi tin nhắn SMS đến các thiết bị di động và nhận tin nhắn SMS từ các thiết bị di động.

-Hiện nay giao thức SMPP đã trở thành giao thức được chấp nhận rộng rãi trong ngành viễn thông để gửi tin nhắn SMS. Nó hoạt động như một phương tiện để gửi các chiến dịch tiếp thị, cập nhật tin tức và cập nhật kinh doanh.



**Các thành phần của SMPP:**

***SMSC( short massage service center): Trung tâm dịch vụ tin nhắn ngắn.***

Chức năng: Là trung tâm xử lý tin nhắn ngắn, chịu trách nhiệm nhận, lưu trữ, định tuyến và gửi tin nhắn SMS đến thiết bị người dùng hoặc các hệ thống khác.

Vai trò trong SMPP: SMSC hoạt động như một máy chủ, kết nối với các ESME để xử lý yêu cầu gửi/nhận tin nhắn.

Ví dụ: Khi bạn gửi SMS, SMSC sẽ lưu tin nhắn nếu người nhận chưa sẵn sàng, sau đó chuyển tiếp khi họ online.

***ESME ( external short messaging entity): Thực thể tin nhắn ngắn bên ngoài***

Chức năng: Là các ứng dụng hoặc hệ thống bên ngoài tương tác với SMSC để gửi hoặc nhận tin nhắn SMS.

Ví dụ: Các cổng SMS của doanh nghiệp (như gửi mã OTP), nhà cung cấp nội dung, hoặc ứng dụng nhắn tin tự động.

Vai trò trong SMPP: ESME kết nối với SMSC thông qua các phiên (bind) để thực hiện giao tiếp.

***PDU (Protocol Data Unit)***

* PDUs là các gói dữ liệu cơ bản được trao đổi giữa ESME và SMSC để thực hiện các hoạt động khác nhau. Mỗi PDU bao gồm một **header** (chứa thông tin về độ dài, ID lệnh, trạng thái lệnh và số thứ tự) và một **body** (chứa các tham số cụ thể cho từng lệnh).
* Các loại PDUs quan trọng bao gồm:
  + **Bind PDUs:** bind\_transmitter, bind\_receiver, bind\_transceiver (yêu cầu thiết lập phiên) và các PDU phản hồi tương ứng (bind\_transmitter\_resp, bind\_receiver\_resp, bind\_transceiver\_resp).
  + **Unbind PDU:** unbind (yêu cầu kết thúc phiên) và unbind\_resp (phản hồi).
  + **Message Submission PDUs:** submit\_sm (gửi tin nhắn từ ESME đến SMSC) và submit\_sm\_resp (phản hồi).
  + **Message Delivery PDUs:** deliver\_sm (gửi tin nhắn hoặc báo cáo trạng thái từ SMSC đến ESME) và deliver\_sm\_resp (phản hồi).
  + **Query PDU:** query\_sm (yêu cầu trạng thái của một tin nhắn đã gửi) và query\_sm\_resp (phản hồi).
  + **Cancel PDU:** cancel\_sm (yêu cầu hủy một tin nhắn đang chờ xử lý) và cancel\_sm\_resp (phản hồi).
  + **Replace PDU:** replace\_sm (yêu cầu thay thế nội dung của một tin nhắn đang chờ xử lý) và replace\_sm\_resp (phản hồi).
  + **Enquire Link PDU:** enquire\_link (kiểm tra xem kết nối còn hoạt động) và enquire\_link\_resp (phản hồi).
  + **Generic NACK PDU:** generic\_nack (phản hồi lỗi chung).

**SMPP được dùng để:**

SMPP là thành phần chính của truyền thông SMS hiện đại và được sử dụng trong nhiều ứng dụng.

Nhắn tin doanh nghiệp sử dụng SMPP để gửi tin nhắn văn bản từ một chương trình phần mềm đến các số điện thoại cá nhân hoặc danh sách hàng loạt. Điều này bao gồm mọi thứ từ tin nhắn tiếp thị đến dịch vụ thông tin, nhắc nhở cuộc hẹn, dịch vụ chatbot và thậm chí cả yêu cầu đặt lại mật khẩu.

Các thiết bị Internet vạn vật di động (IoT) như đồng hồ đo thông minh sử dụng SMPP để truyền thông tin cập nhật về mức tiêu thụ tài nguyên và trạng thái vị trí. Khi một sự kiện như đột nhập hoặc hỏa hoạn kích hoạt hệ thống báo động thông minh, nó sẽ sử dụng SMPP để nhắn tin cho chủ sở hữu tòa nhà, có khả năng có liên kết cho phép họ truy cập nguồn cấp dữ liệu camera.

**SMPP hoạt động là:**

SMPP hoạt động theo mô hình máy khách-máy chủ, trong đó ESME đóng vai trò là máy khách và SMSC đóng vai trò là máy chủ .

Giao thức này tạo điều kiện thuận lợi cho giao tiếp hai chiều , cho phép gửi tin nhắn (thiết bị di động kết thúc – MT) và nhận tin nhắn (thiết bị di động bắt đầu – MO) thông qua nhiều hoạt động khác nhau. Giao thức này được thiết kế để hoạt động trên các giao thức mạng TCP/IP, đảm bảo việc phân phối tin nhắn đáng tin cậy, có thứ tự và được kiểm tra lỗi qua mạng.

Trước khi trao đổi bất kỳ tin nhắn nào, lệnh bind phải được gửi và xác nhận. Lệnh bind xác định hướng nào có thể gửi tin nhắn; bind\_transmitter chỉ cho phép máy khách gửi tin nhắn đến máy chủ, bind\_receiver có nghĩa là máy khách sẽ chỉ nhận được tin nhắn và bind\_transceiver cho phép truyền tin nhắn theo cả hai hướng. Trong lệnh bind, ESME tự xác định chính nó bằng system\_id, system\_type và password; trường address\_range được thiết kế để chứa địa chỉ ESME thường được để trống. Lệnh bind chứa tham số interface\_version để chỉ định phiên bản giao thức SMPP nào sẽ được sử dụng.

Trao đổi tin nhắn có thể đồng bộ, trong đó mỗi bên chờ phản hồi cho mỗi PDU được gửi hoặc không đồng bộ, trong đó nhiều yêu cầu có thể được đưa ra mà không cần chờ và được bên kia xác nhận theo thứ tự lệch; số lượng yêu cầu chưa được xác nhận được gọi là một *window* ; để có hiệu suất tốt nhất, cả hai bên giao tiếp phải được cấu hình với cùng window size.

Sau đây là một ví dụ về cách SMPP thường hoạt động trong thực tế:

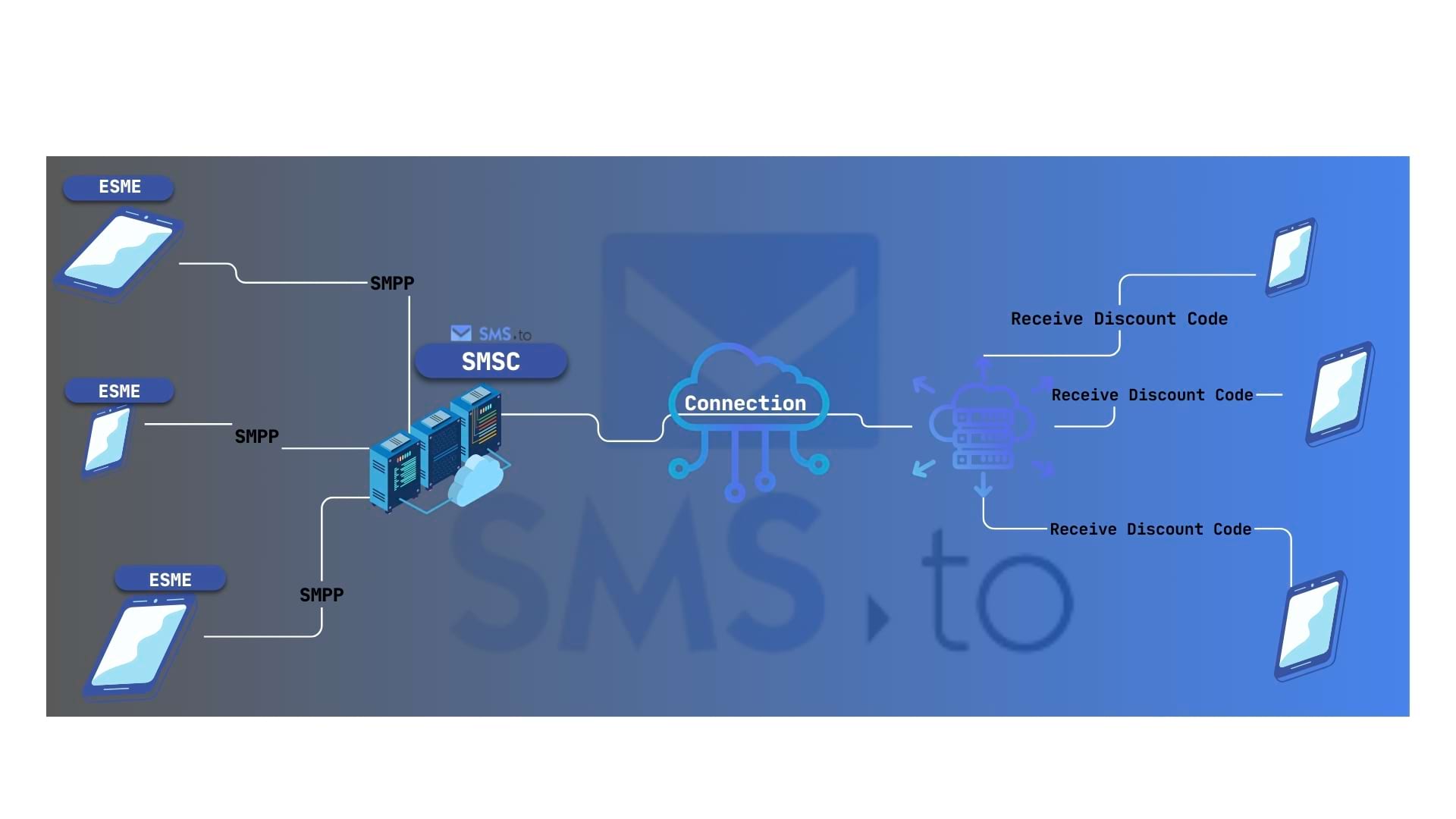
Ví dụ bạn đang gửi tin nhắn văn bản từ ứng dụng của quán cà phê yêu thích để nhận được giảm giá. SMPP hoạt động trong trường hợp này là:

Bạn yêu cầu giảm giá : Bạn chạm vào “Gửi cho tôi mức giảm giá!” trong ứng dụng.

Liên hệ ứng dụng SMSC : Ứng dụng của quán cà phê, hoạt động như một ESME, sử dụng SMPP để gửi yêu cầu của bạn đến SMSC của mạng di động.

SMSC gửi tin nhắn SMS của bạn : SMSC nhận được yêu cầu và gửi tin nhắn văn bản có mã giảm giá đến điện thoại của bạn.

Bạn nhận được tin nhắn SMS giảm giá : Điện thoại của bạn nhận được tin nhắn với mã giảm giá cho ly cà phê!



**Có những nguy cơ bất thường là:**

-Các vấn đề và lỗi kết nối : Trong quá trình truyền tin nhắn từ nhà mạng này sang nhà mạng khác, có thể có những sự cố có thể gây trở ngại cho quá trình này. Những sự cố này xuất hiện dưới dạng lỗi như số lượng từ SMS vượt quá hoặc người nhận không hợp lệ.

Ngoài ra, giao thức SMPP không phù hợp với kết nối công cộng. Sử dụng mạng công cộng để gửi tin nhắn SMS bằng giao thức SMPP sẽ ngăn chặn mức độ bảo mật và kiểm soát thường được yêu cầu đối với các ứng dụng nhắn tin cấp doanh nghiệp hoặc cấp độ quan trọng.

Để tránh lỗi SMPP, hãy đảm bảo bạn nhập đúng ID cho người nhận và không vượt quá giới hạn số lượng từ. Ngoài ra, bạn nên sử dụng kết nối riêng tư chuyên dụng khi thiết lập giao thức SMS SMPP để đảm bảo kết nối ổn định.

-Chọn nhà cung cấp SMPP phù hợp : Một trong những vấn đề thường gặp mà doanh nghiệp gặp phải khi sử dụng SMPP là chọn nhà cung cấp SMS SMPP tốt.

Quá trình này rất quan trọng vì nhà cung cấp của bạn sẽ quyết định mức độ hiệu quả của quá trình truyền tải tin nhắn.

-Mối lo ngại tiềm ẩn về bảo mật : Mặc dù giao thức SMPP không được trang bị cấu trúc bảo mật , ta vẫn có thể thiết lập các biện pháp để đảm bảo tin nhắn của mình được an toàn.

Ví dụ, ta có thể tích hợp SMPP với Transport Layer Security (TLS), một kênh mã hóa đảm bảo tính riêng tư và toàn vẹn của tin nhắn.

TLS bao gồm một cơ chế xác thực máy chủ, giúp các máy khách SMPP xác minh danh tính của máy chủ mà chúng đang kết nối. Điều này ngăn chặn các cuộc tấn công trung gian, trong đó kẻ tấn công mạo danh máy chủ SMPP để chặn hoặc thao túng tin nhắn. Xác thực máy chủ dựa trên các chứng chỉ kỹ thuật số do các cơ quan cấp chứng chỉ (CA) đáng tin cậy cấp.

-Vấn đề về hiệu suất:

Quá tải hệ thống: Nếu ESME gửi quá nhiều tin nhắn cùng lúc mà không tuân theo giới hạn "window size" của SMPP, SMSC có thể từ chối hoặc trì hoãn xử lý.

Độ trễ cao: Khi mạng chậm hoặc SMSC xử lý không kịp, tin nhắn có thể bị giao chậm, ảnh hưởng đến trải nghiệm người dùng.

-Lỗi xử lý tin nhắn: Nếu SMSC hoặc ESME không quản lý tốt Message\_ID, tin nhắn có thể gửi hoặc nhận nhiều lần.; Trong trường hợp SMSC bị lỗi hoặc mạng không ổn định, tin nhắn có thể bị rơi mà ko có thông báo; Với tin nhắn dài nếu không cấu hình đúng nội dung có thể bị cắt xén hoặc hiển thị sai.

-Rủi ro pháp lý và tuân thủ: Nếu ESME gửi SMS spam hoặc nội dung vi phạm pháp luật hệ thống có thể bị phạt ; Một số quốc gia yêu cầu lưu trữ tin nhắn để kiểm tra. Nếu không tuân thủ, có thể gặp rủi ro.

**Cấu trúc tấn công giao thức SMPP**

1. **Thu thập thông tin**

* Mục tiêu: Xác định mục tiêu SMSC hoặc ESME, bao gồm địa chỉ IP, cổng, và thông tin xác thực
* Cách thực hiện:
* Quét mạng bằng công cụ như nmap để tìm các cổng SMPP mở (thường là 2775).
* Thu thập thông tin từ tài liệu công khai, cấu hình sai của hệ thống, hoặc nghe lén lưu lượng mạng (nếu không mã hóa).
* Đặc trưng SMPP:
* Giao thức không yêu cầu mã hóa mặc định, nên dữ liệu như system\_id và password trong PDU bind\_transmitter có thể bị chặn nếu kênh truyền ko dùng SSL/TLS.
* Kết quả:
* Kẻ tấn công có danh sách mục tiêu và thông tin cơ bản để lập kế hoạch.

1. **Thiết lập kết nối**

* Mục tiêu: Kết nối SMSC hoặc ESME để bắt đầu gửi PDU
* Cách thực hiện:
* Sử dụng client SMPP giả lập để gửi PDU bind\_Transmitter hoặc bind\_reciver
* Nếu không có thông tin xác thực hợp lệ, kẻ tấn công sẽ vượt qua giai đoạn xác thực.
* Điểm yếu SMPP:
* Xác thực dựa trên system\_id và password dạng plaintext trong body của PDU.
* Không có cơ chế bảo vệ chống đoán mật khẩu( brute force) nếu SMSC không giới hạn số lần thử.

1. **Khai thác**

* Mục tiêu: Thực hiện hành vi độc hại dựa trên các loại tấn công.
* Kịch bản của các loại tấn công:

1. *Tấn công DoS*

- Gửi liên tục PDU submit\_sm với nội dung tin nhắn giả để làm quá tải SMSC.

- Cấu trúc PDU:

Header: command\_id = 0x00000004 (submit\_sm), sequence number tăng nhanh.

Body: Số điện thoại giả, nội dung tin nhắn dài bất thường để tiêu tốn tài nguyên.

1. *Spoofing ( Giả mạo )*

Gửi tin nhắn giả mạo từ một nguồn hợp lệ (e.g., ngân hàng, nhà mạng).

Cấu trúc PDU: submit\_sm với trường source\_addr giả mạo.

1. *Replay Attrack*

Ghi lại submit\_sm hợp lệ, thay đổi sequence\_number, gửi lại nhiều lần.

1. *Thay đổi dữ liệu*

Chặn và sửa đổi PDU trong quá trình truyền (nếu không mã hóa), thay đổi nội dung tin nhắn hoặc số điện thoại.

Cấu trúc: Body của PDU bị chỉnh sửa (e.g., thay đổi short\_message).

* Điểm yếu của SMPP:
* Thiếu kiểm tra tính toàn vẹn dữ liệu.
* Không có cơ chế chống lặp lại PDU (nonce/time-based validation).
* Xử lý đầu vào không chặt chẽ có thể gây lỗi (e.g., tràn bộ đệm nếu SMSC không kiểm tra độ dài).

1. **Duy trì**

* Mục tiêu: Duy trì ảnh hưởng hoặc tăng cường hiệu quả tấn công.
* Cách thực hiện:
* Duy trì nhiều kết nối TCP song song để gửi PDU liên tục.
* Sử dụng botnet để phân tán nguồn tấn công, làm khó phát hiện và chặn.
* Đặc trưng SMPP: Một khi phiên (bind) được thiết lập, kẻ tấn công có thể gửi hàng loạt PDU mà không cần xác thực lại, nếu SMSC không giới hạn truy cập.

1. **Che giấu dấu vết**

* Mục tiêu: Tránh bị phát hiện hoặc truy vết.
* Cách thực hiện:
* Sử dụng VPN hoặc proxy để che giấu địa chỉ IP.
* Ngắt kết nối ngay sau khi tấn công, không để lại log trên hệ thống tấn công.
* Điểm yếu SMPP: Giao thức không yêu cầu xác minh nguồn gốc mạnh, nên việc truy vết phụ thuộc vào SMSC.

**Tài liệu tham khảo thêm**

1. <https://mo.co.za/open/silentdos.pdf>
2. <https://www.ijsr.net/archive/v4i7/SUB157022.pdf>
3. <https://www.researchgate.net/publication/220383835_Threats_and_Countermeasures_in_GSM_Networks>.

Cơ chế, kết cấu