DATE

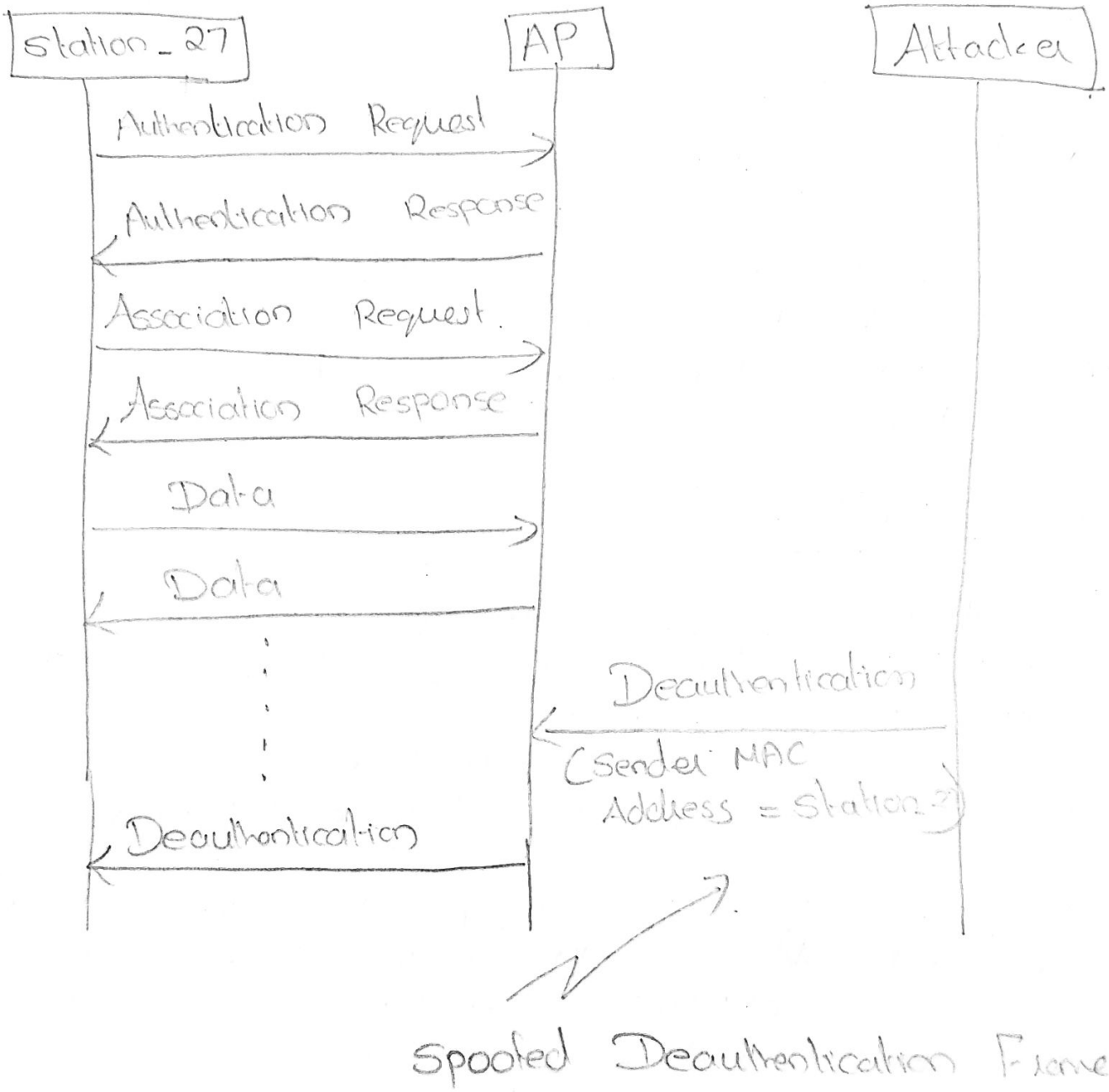
Wireless LAN Vulnerabilities

The MAC (Medium Access Control) controls the access to the shared medium in a LAN.
The smooth functioning of these n/w depends on the stations on the LAN strictly obeying the rules.

Frame Spoofing

A station needs to authenticate and then associate with an AP before they can exchange the data frame b/w each other.
Either party can at any point in time, terminate the connection by transmitting a "Deauthentication Frame."
The recipient of a mangement frame relies on the Sender Address field in the frame to identify the originator of the message. However an attacker can spoof (pretend to be the ~~send~~ actual sender) the Sender Address in the frame.
eg he can fabricate a Deauthentication frame with

Sender Address = Station - 27
Receiver Address = AP



- The address is a 48-bit MAC address.
- When AP receives the above frame, it thinks tha Station_27 wishes to terminate the existing connection.
- The AP sets the state of the connection b/w itself and station_27 to be "Unauthenticated and Unassociated"

Station_27 would have to go theough the time-consuming process of re-authenticating and re-associating itself to the AP if it wishes to resume the connection.

The attacker could repeatedly transmit such Deauthentication frames to the AP thus effectively slowing down or even preventing communications blw station_27 and the AP.

Spoofing Power Management Control Frames

A mobile station typically works on batteries.

To save power, a mobile station powers off its transceiver. It informs the AP that it is in power-saving mode so that the AP can buffer all frames intended for it.

When the station wakes up, it informs the AP that it is in the active state using a Poll Control Frame.

On receipt of the Poll Control Frame, the AP delivers the station any frames that it had buffered for it while the station was in the power-saving mode.

- An attacker could spoof Poll control frames and make it appear that they were sent by a sleeping station that has just woken up.
- The AP on receiving the spoofed Poll control frame could deliver the buffered frames to the sleeping station.
- But since the receiver of the sleeping station is powered off, the frames cannot be captured by the sleeping station.
- When the sleeping station actually wakes up it may send Poll Control frame to receive the buffered frames. Since all the buffered frames were already transmitted by the AP. (no copy is maintained after transmission), it will not receive the frames destined for it while it was asleep.

DATE

Page No 11

Cellphone Security

Global System for Mobile Communications (GSM) or 2G goals were better quality for voice, higher speeds for data, and other non-voice applications and international roaming.

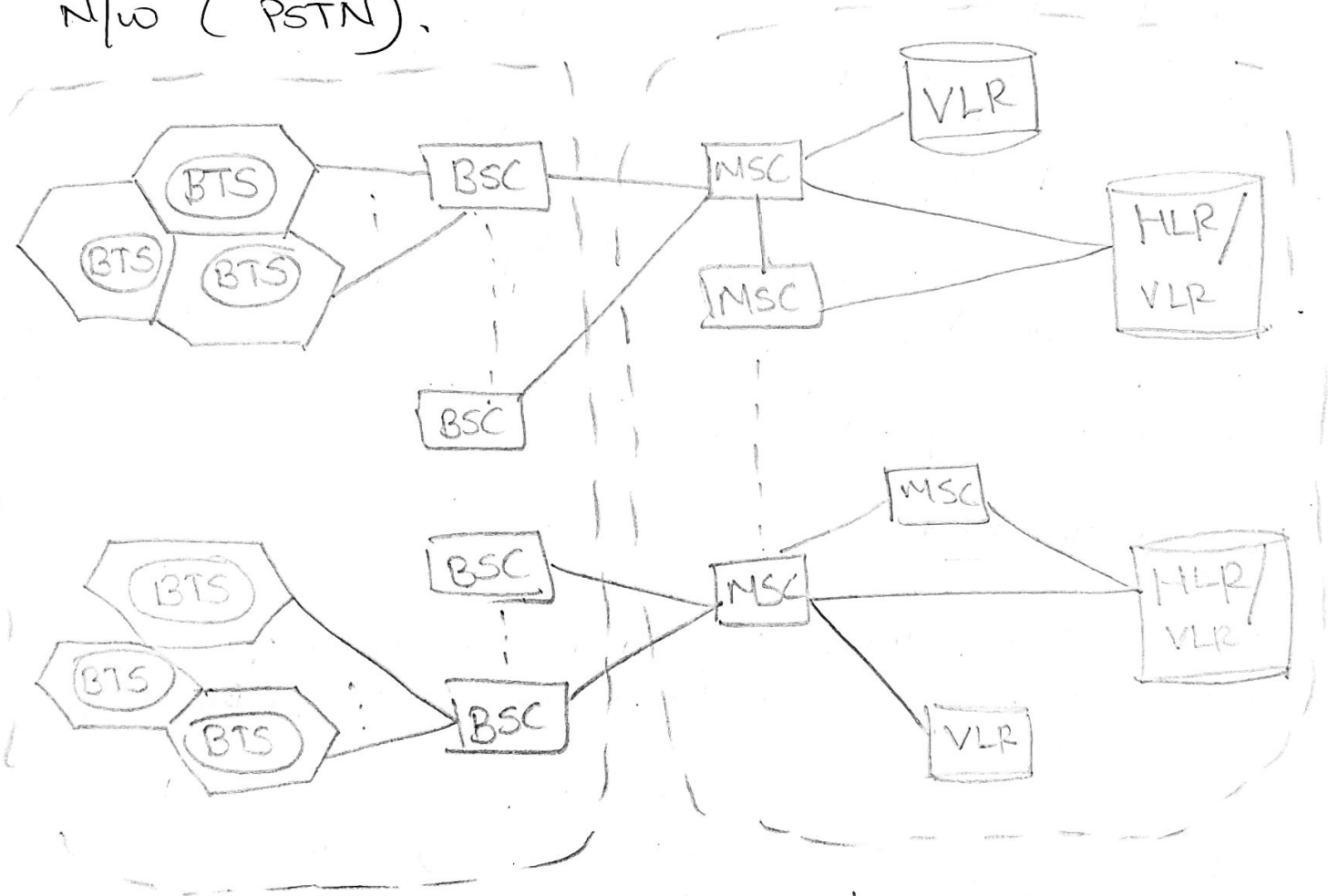
- The successor of GSM is Universal Mobile Telecommunications System (UMTS) or 3G it features are advanced service such as mobile Internet, multimedia messaging, videoconferencing etc.

Entities Involved

- At the lowest level a cellphone is connected to a base station or base transceiver station (BTS) by a radio link.
- Multiple base stations are connected to and controlled by a base station Controller (BSC). The connection b/w base station and BSC is done through microwave link, optical link etc.
- Multiple BSC are connected to a Mobile switching center (MSC). The MSC forwards an incoming call to the MSC where the call recipient is located. The MSC also handles

call billing and accounting functions.

- MSCs are connected to each other through wired n/w such as the Packet switched Telephone N/w (PSTN).



- A user's home n/w is the one with whom the user has a subscription.
- There is a one-to-one mapping b/w a n/w and an MSC.

- An MSC has a DB called the Home Location Register (HLR), containing information about each of its subscribers. This includes static information such as the subscribers mobile no, services subscribed to, and a secret key stored in the mobile and known only to the HLR.

- The HLR also contains dynamic information for each of its roaming subscribers. This includes the current location of a subscriber, i.e the cellular n/w the user may be currently visiting.

- A subscriber may avail the services of other n/w that have a roaming agreement with the subscriber's home n/w.

- Each cellular n/w also maintains a DB of users currently visiting that n/w together with the list of services the subscriber is entitled to. This DB is the Visital Location Register (VLR)

Security Goals

1. User Identity confidentiality - One way for a eavesdropper to identify a caller is through the

IMSI transmitted by the cellphone when a call is made. To protect the user's privacy, GSM requires that the IMSI should be used rarely. eg during initial authentication to a foreign n/w.

[Subscriber Identity Module (SIM) its a smart card it stores 3 secrets and performs cryptographic operations involving some of the secrets. The secrets are

a) a unique 15-digit subscriber identification number called the International Mobile Subscriber Identity (IMSI)
b) a 128-bit subscriber authentication key denoted Ki known only to the SIM and the HLR of the subscriber's home n/w
c) a PIN known to the phone's owner and used to unlock the SIM]

2. Temporary Mobile Subscriber Identity (TMSI) - is assigned to a user. This has limited-time validity, only within a particular n/w. When a user changes location and moves to a new n/w the user's cellphone will have to be re-authenticated and a new TMSI is assigned.

The mapping b/w the cellphone's TMSI and its IMSI is maintained in the VLR.

IMSI - is a fixed subscriber ID

TMSI - is a random integer and its use is temporary. Hence TMSI is used instead of IMSI to prevent the tracking of cellphone users.

3. Message Confidentiality.

4. Entity authentication - The MSC needs to be sure that the call is billed to the person making the call. The caller needs to convince itself that it is talking to the genuine base station.

5. Message Origin Authentication and message integrity -

For each signalling msg b/w the cellphone and base station the recipient needs to verify that the msg has been received without error. Both the parties should be able to verify that each msg was created by the party at the other end and not by the attacker.