Security for Mobile IP in the 3G Networks

Pat R. Calhoun
Network and Security Center
Sun Microsystems, Inc.

Introduction

- This presentation will detail some of the current cellular architectures, and their security requirements and designs.
- I will also provide some insight on the current security model being considered in 3GPP2/TIA architectures.

Introduction – SDO's

- The information that I will present come from three different cellular standards (or standards setting) groups:
  - Telecommunications Industry Association (TIA). www.tiaonline.org
  - 3rd Generation Partnership Project Number 2 (3GPP 2). www.3gpp2.org
  - Mobile Wireless Internet Forum (WMIF). www.mwif.org

Introduction – SDO's

- The TIA and 3GPP2 architecture and requirements stated in this presentation apply to CDMA networks only.
- MWIF is a group that is attempting to define a consistent architecture for both 3GPP2 (CDMA) and 3GPP (GSM) networks. MWIF is not an SDO.

Disclaimer

- The ramblings found in this presentation are my own interpretation of the work in progress. I am **not** representing the SDOs.
- Note that in some cases, the presenter does not necessarily agree with the design decisions (please, don't shoot the messenger).

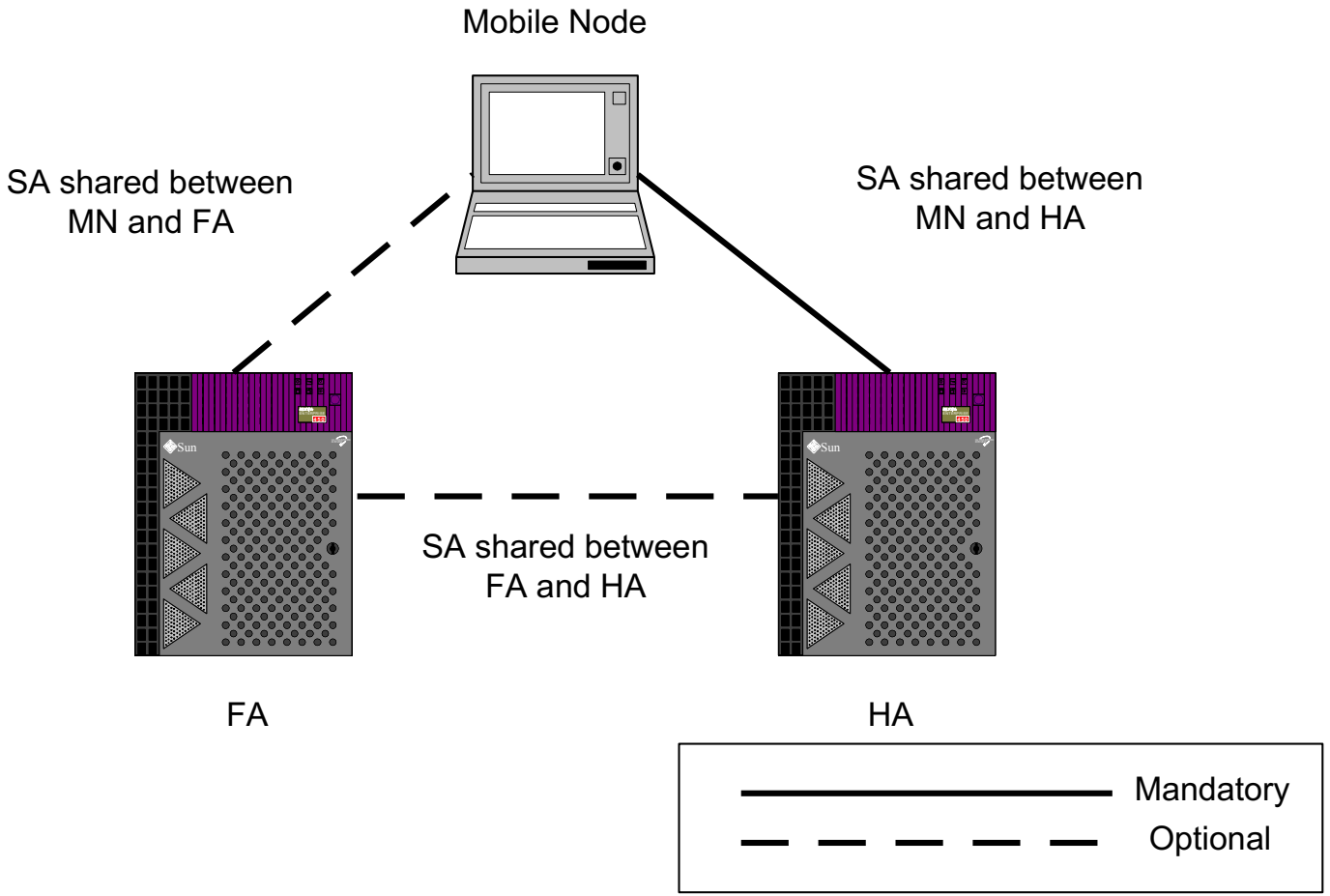
3GPP2 – TSG-P

- The 3rd Generation Partnership Project 2 (3GPP2) TSG-P Working Group is responsible for creating the data architecture components of the 3rd generation CDMA network.
- The WG made a conscious decision to base as much as it could of its architecture on IETF protocols.

Legacy Mobile IP Trust Model

- Mobile IP, as defined in RFC 2002, requires that a Mobile Node share a static security association (SA) with its Home Agent.
- The protocol also allows the Mobile Node to share an SA with Foreign Agents, which in turn can share SAs with Home Agents

Mobile IP Trust Model



Mobile IP Trust Model

- When all three entities use authentication, a N x N number of security associations is required.
- This problem becomes much more important in inter-domain mobility scenarios.
- In 3G networks, the optional Mobile IP authentication extensions (MN-FA, FA-HA) are used.

Interim Security Solution

- Due to the fact that AAA standards aren't available today, TSG-P's interim solution involves RADIUS.
- When a Mobile Node is authentication, the RADIUS server includes a long-lived key to be used with the Foreign Agent to authentication messages with the Home Agent.

Interim Security Solution[1]

- The Foreign Agent uses the long lived key to secure messages with the Home Agent.
- This means that any Foreign Agent on the ‘net that has a valid (authenticated) Mobile Node will get access to the long lived key!!
- There is no authentication between the Mobile Node and the Foreign Agent.

[1] of lack thereof

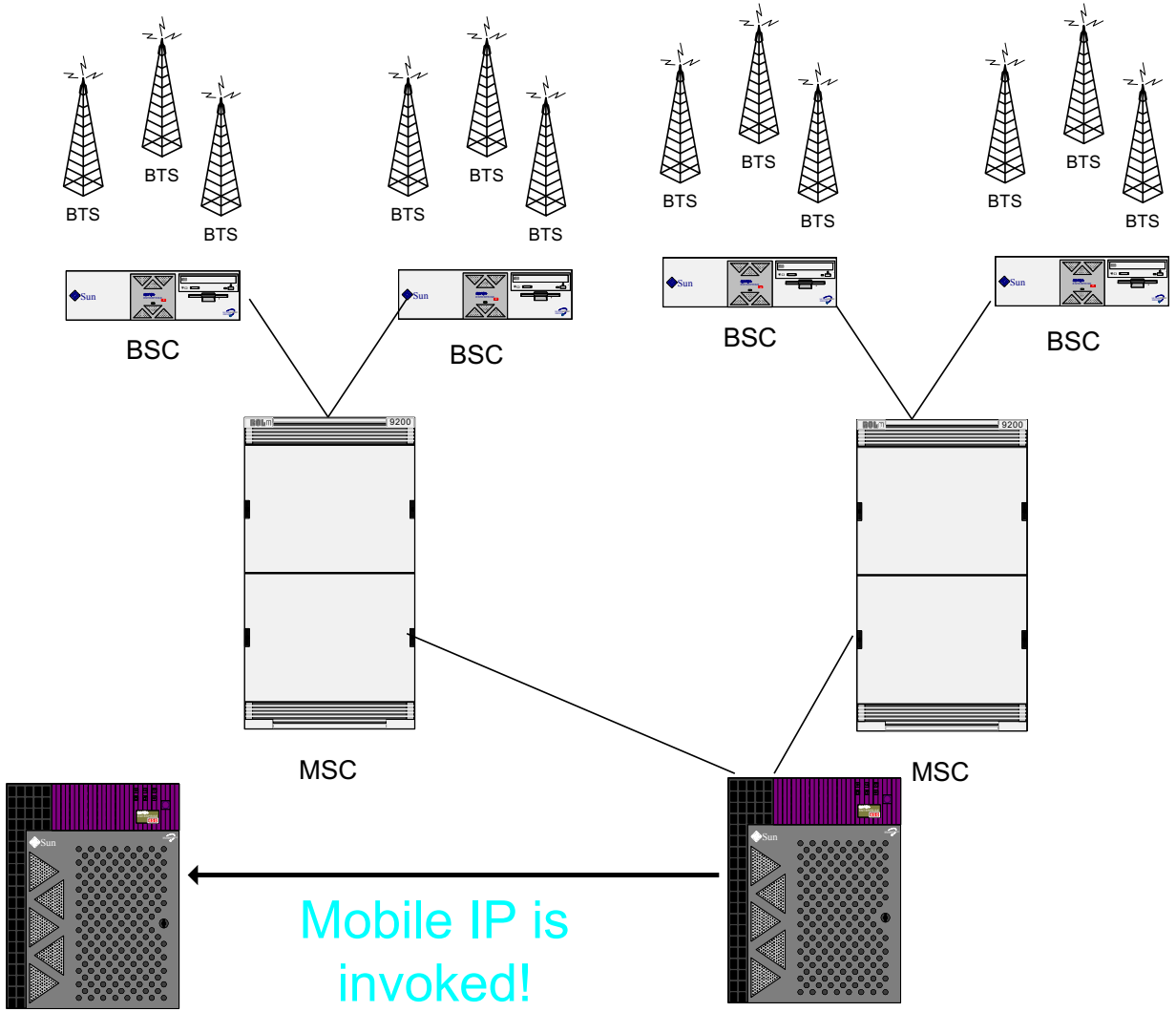
Interim Security Solution

- The interim solution requires that the RADIUS server be contacted for every hand-off, and re-registration, increasing the hand-off latency.

Legacy Hand-off Performance

- When all Mobility entities share static security associations, the latency imposed by a hand-off process can be very small.
- Hand-off performance is very important for the cellular carriers, as they expect to provide a service that is at least equivalent to today's service.

Hand-off in TSG-P network



Triangular Route

- Mobile IP introduces a triangular route for traffic destined for the Mobile Node.
- The farther (topologically) the Mobile Node moves away from its Home Agent, the longer the latency in packet delivery.

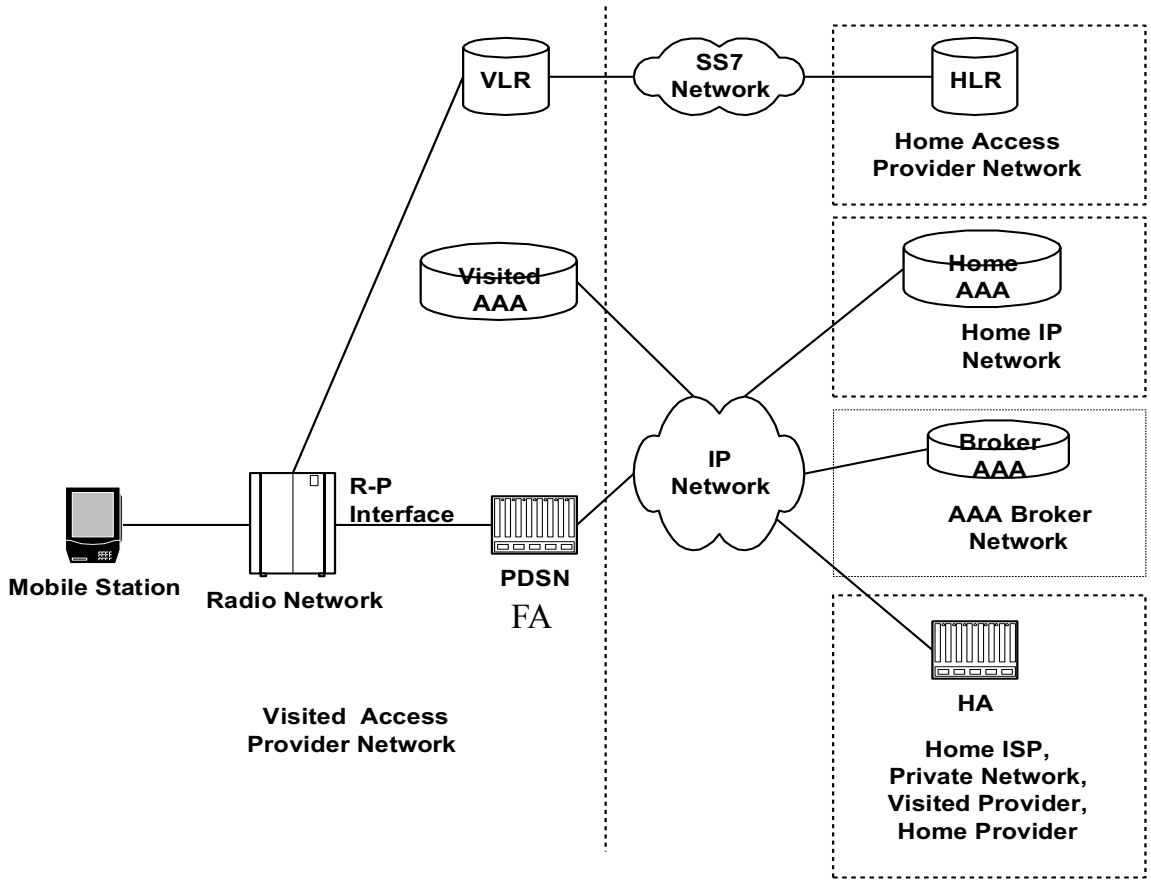
TSG-P Hand-off Solution

- Route Optimization is still considered as a “research topic” by the cellular carriers, so they require a Mobile Node to be assigned a dynamic Home Agent.
- When the Mobile Node initially registers, a Home Agent that is topologically near the MN is assigned.
- The farther the MN moves away, the larger the triangular route.

TSG-P Hand-off Solution

- The TSG-P architecture document also allows the Mobile Node to have a Home Agent assigned in a visited domain, which is a big departure from RFC2002.

TSG-P Architecture

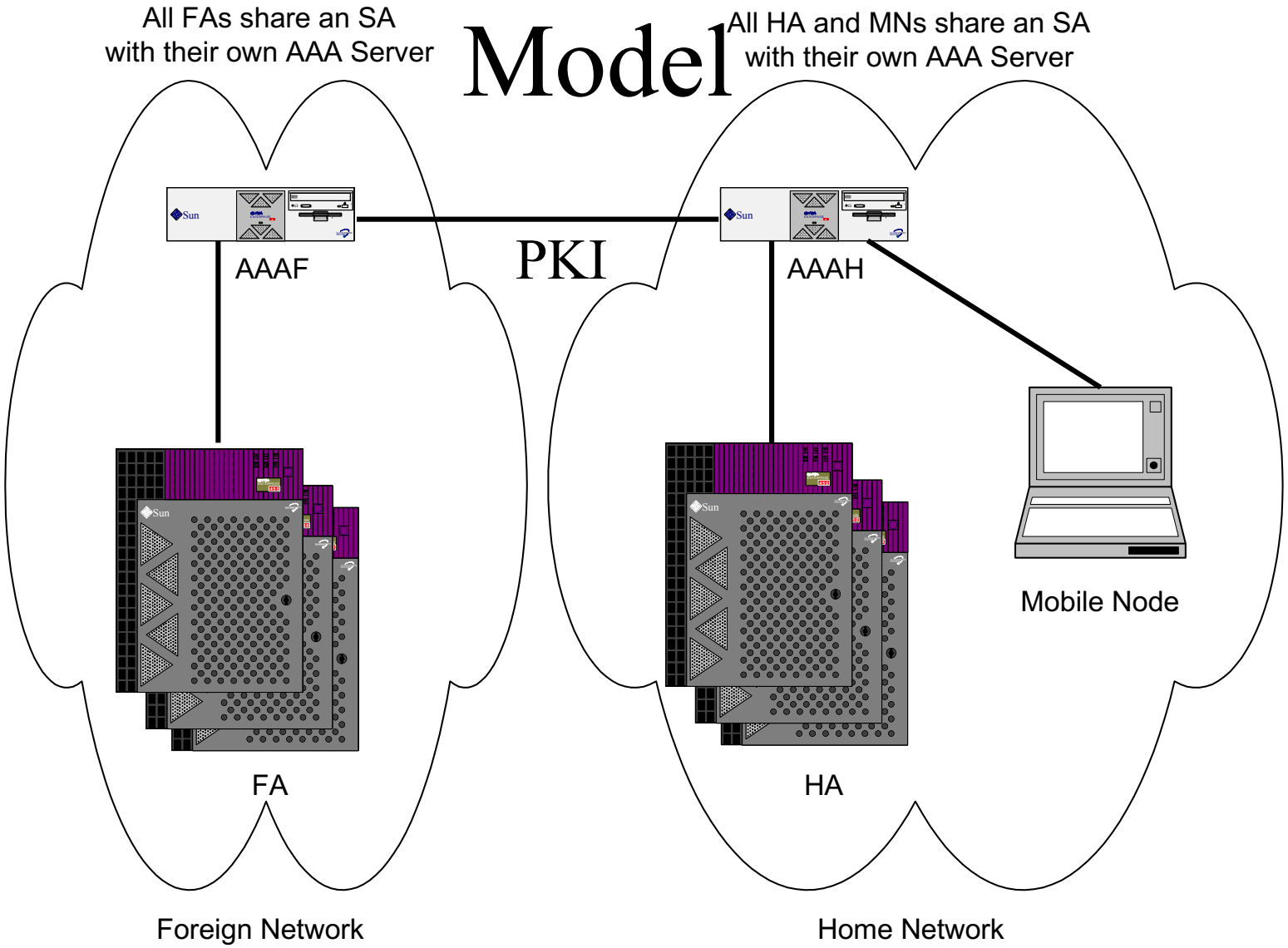


Source: TSG-P Standards baseline architecture specification.

AAA/Mobile IP Trust Model

- TSG-P has adopted an architecture where all Mobile Nodes share a security association with their respective Home AAA Servers (AAAH).
- Furthermore, all Mobility Agents share a security association with their own AAA Server(s).

Proposed Mobile IP/AAA Trust Model

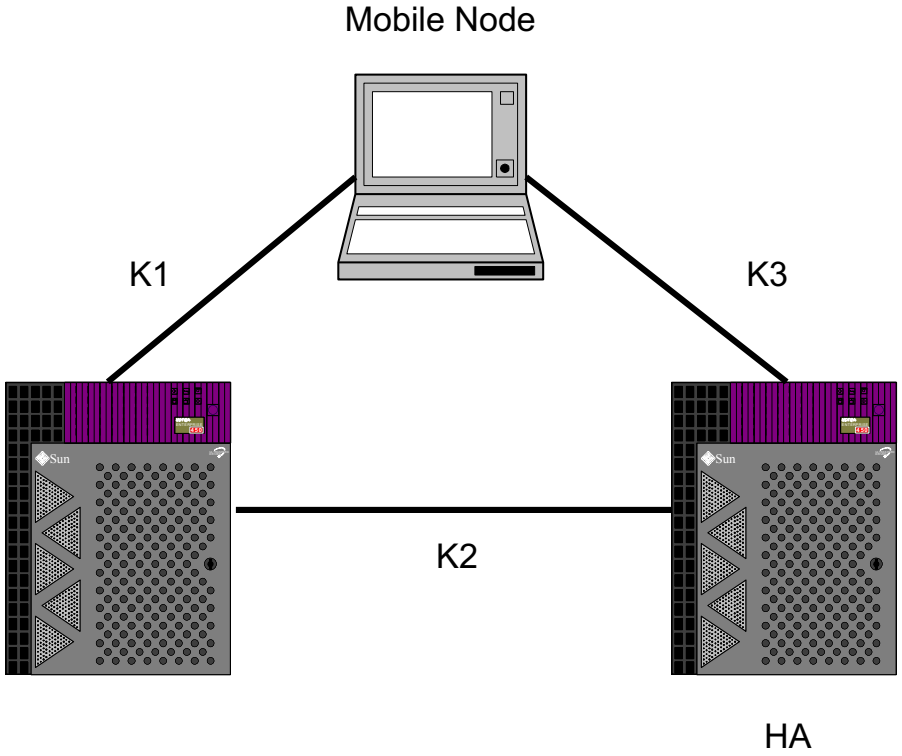


AAA/Mobile IP Trust Model

- As previously noted, TSG-P's architecture requires the three way SA for Mobile IP message authentication.
- When successfully authenticated, the AAAH creates three encrypted keysets[1]:
  - K1: MN-FA keyset
  - K2: FA-HA keyset
  - K3: MN-HA keyset

[1] May use symmetric or asymmetric cryptography

AAA/Mobile IP Trust Model



When the keysets are distributed, the Mobile IP messages are authenticated using the new keys.

AAA/Mobile IP Trust Model

- The keysets have a lifetime, and can be used to authenticate all Mobile IP messages until they expire.
- The Mobile IP registration normally expires well before the keysets expire, allowing the keys to be re-used.
- The AAA infrastructure only need to be contacted when the keys expire, or when the Mobile Node enters a new domain.

Advantages

- The dynamic Security Association proposal assumes that all mobility entities inherently trust their AAA servers.
- The registration and key distribution occurs in a single round trip (it is assumed that the AAA servers communicate frequently enough that they already have each other's validated certificates).
- The PKI is still used in the network, but mostly where trust is weak, such as in Inter-Domain communication.

IKE and Mobile IP

- The question that comes to mind is why aren't we using IKE to secure Mobile IP messages?
- if Mobile Node has a static IP address, IKE could be run between the Mobile Node and the Foreign Agent, and between the Foreign Agent and the Home Agent.

IKE and Mobile IP

- One problem is that Mobile IP isn't IKE-compatible (for MN-HA Mobile IP message authentication), since the Mobile IP messages are processed at the application layer by the Foreign Agent.

IKE Issues

- The cellular carriers haven’t seriously considered IKE to protect the Mobile IP messages due to the large overhead required in order to setup the IKE Security Association (large number of round trips).

Route Optimization

- The real solution is route optimization, but this requires a whole security infrastructure.
- This could be achieved for cellular devices, but land-line devices would also need to be part of the security infrastructure.
- Without it, real-time applications in cellular networks is difficult to do.

Data Privacy

- Since the Mobile Node is connected to the network, end-to-end security may be used via IP Security or some other security mechanism.
- Note that the data is protected over the air (just how secure this really is, is subject to a longer discussion).

Data Privacy

- One of TSG-P's main goal is to provide enterprise network access.
- Ideally, the mobile's traffic would be secured end-to-end.
- TSG-P decided to provide a feature that allows the data to be encrypted by the PDSN towards the Home Agent.

Data Privacy

- The data is in the clear between the RAN and the PDSN, but it is encrypted over the air[1].
- This minimizes the per-packet overhead over the air.

[1] The author would like to request that any flames be directed to 3GPP2.

End-to-End Security

- If one is willing to live with the IP Security per-packet overhead, or use end-to-end TLS, Mobile IP offers some advantages.
- Since the Mobile's IP address doesn't change during a hand-off, the existing IKE Sas (or TLS sessions) can be re-used.

Header compression and Security

- Since end-to-end security is desired, doing so eliminates many of the advantages of header compression over the air.

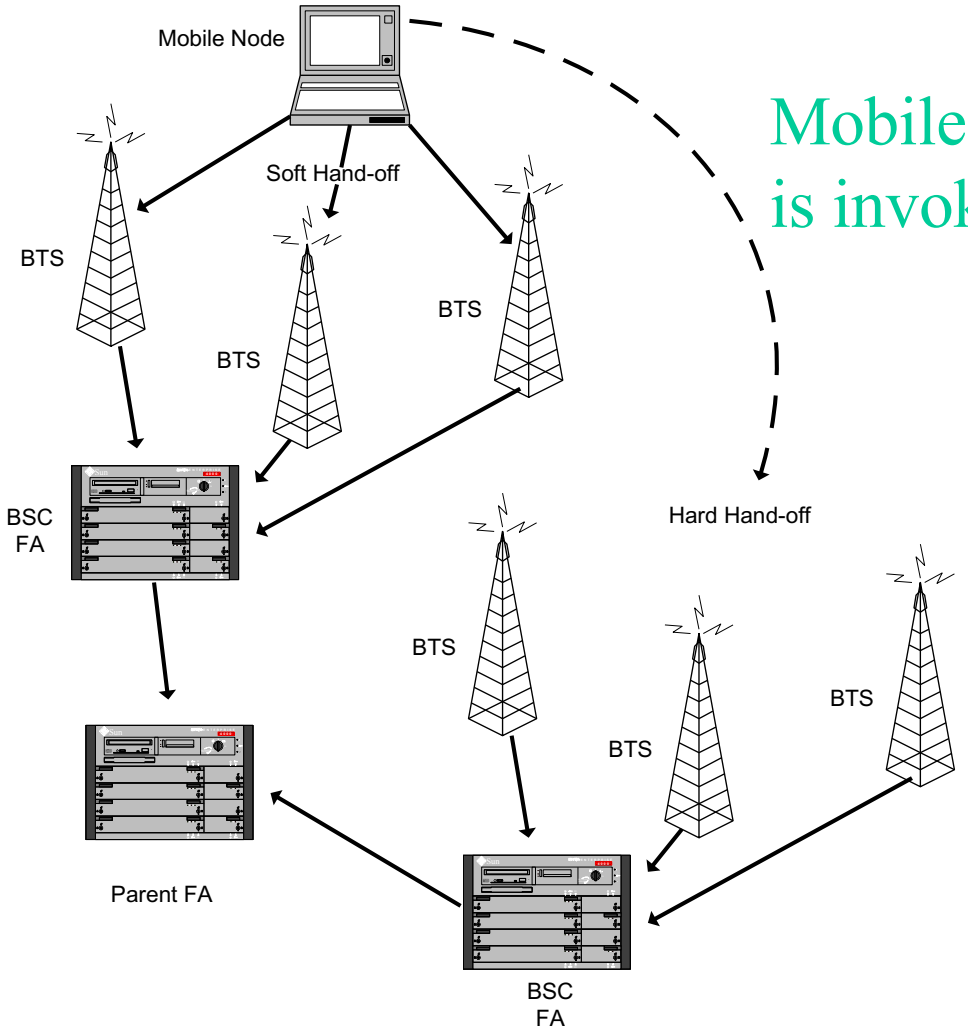
3GPP2 All-IP Ad-Hoc

- 3GPP2 recently formed an ad-hoc committee that is responsible for defining the architecture for an All-IP cellular network.
- What All-IP is, and where IP resides in the network, is still in question, but many people believe that IP should be moved down to the base station.

All-IP Architecture

- The All-IP group is not only concerned with IP-enabled mobiles, but also the legacy voice-only devices.
- Mobility Management is a big component of the cellular network, and it seems as if Mobile IP may be the right protocol for the job.
- Mobile IP would be moved as close as possible to the Base Station Controller as possible

Hand-off in All-IP network



Mobile IP
is invoked!

Hand-off in All-IP network

- In the All-IP network, hand-off that involve Mobile IP are much more frequent, so the additional latency involved in securing the messages become even more of an issue.
- The carriers want to provide a service that is at least equivalent to the service customers get today. This is especially noticeable for voice services.

Hand-off in All-IP network

- The registration process during a hand-off still needs to be authenticated.
- Again, an optimized key distribution approach is desired by the cellular carriers.

The future of the HLR

- TSG-P's architecture introduces a duplicate AAA path. AAA for IP-based terminals, and IS-41 for legacy (voice) devices.
- There is some interest in the All-IP networks to move away from the HLR, and make use of AAA for all devices.
- A gateway function would be needed to communicate with legacy (SS7) networks.

Cellular Standards Issues

- Although the cellular standards bodies are willing to adopt IETF-standardized protocol, they have many concerns about our ability to deliver.
- Today's Working Groups have charters that include milestones, but these milestones rarely observed, and seldom is any effort done to meet them.

Conclusions

- The Mobile IP WG must complete its work to bind Mobile IP and AAA.
- If we want to remove Triangular routing introduced by Mobile IP, we need to work on the security infrastructure that is required.

Conclusions

- The AAA Working Group must complete its requirements, and begin the protocol design phase.
- Future AAA work may be necessary to support the legacy devices. This MAY be better handled by the cellular SDOs.

Conclusions

- The cellular carriers would like to make use of a standardized security service, but IKE imposes too much of an overhead. The IETF could investigate if a security service that imposes a lower latency in the hand-off process.