Appendix A

HPLMN IP Services in 3GPP-WLAN

In this appendix, we present a simplified version of the roaming security architecture for access to IP services provided by the HPLMN in 3GPP-WLAN. The functionality of the components used in this architecture are same as the components used in the roaming architecture for access to IP services provided by the VPLMN in 3GPP-WLAN (Chapter 5, Figure 5.1). Here, the difference is that the PDG, with which the UE establishes a tunnel, is located in the HPLMN instead of the VPLMN.
Figure A.1: Simplified roaming security architecture for access to IP services provided by HPLMN in 3GPP-WLAN.
Appendix B

HPLMN IP Services in Non3GPP-EPS

In this appendix, we present a simplified version of the roaming security architecture for access to IP services provided by the HPLMN in Non3GPP-EPS. The functionality of the components used in this architecture are same as the components used in the roaming architectures for access to IP services provided by the VPLMN in Non3GPP-EPS (Chapter 5, Figure 5.2). Here, the difference is that the PDN Gateway is located in the HPLMN instead of the VPLMN. And, an additional component called Serving Gateway (SGW) is used in the VPLMN. The role of SGW is to route user data packets.
Figure B.1: Simplified roaming security architecture for access to IP services provided by HPLMN in Non3GPP-EPS.
Appendix C

Rules of AUTLOG

In this appendix, we present some of the rules of AUTLOG calculus [59] which are used in the formal analysis of Chapter 6, Section 6.2. The symbols that are used in defining these rules along with their usage are as follows (more details about these symbols can be found in [59]):

- \( P, Q, R \) represents agents, who communicate with each other.
- \( M \) represents messages which could be one of the following: names of agents, key components, computed messages, list of messages and derived keys.
- \( M_P \) represents a message in view of \( P \) or in other words a message that is localised towards \( P \). Here, \( P \) does not necessarily understand \( M_P \). For example, \( P \) receives a list including a cryptogram and a hash value: \( P \) sees \( \{X\}_K, h(M) \), where \( P \) cannot decrypt the ciphertext but knows \( M \).
- \( X, X_i, Y, Y_i, Z \) represents messages which could be one of the following: names of agents, key components, computed messages, list of messages, derived keys and localised messages (\( M_P \)).
- \( K \) represents a public key scheme that consist of a public component \( K^+ \) and a private component \( K^- \).
Appendix C. Rules of AUTLOG

- $K^{-1}$ represents an inverse key which is the corresponding component for public key schemes and equal to $K$ in symmetric case.

- $h$ denotes all hash functions including message authentication codes.

- $\sigma$ denotes signatures without message recovery.

- $\text{enc}(K, M) = \{M\}_K$ denotes encryption of a message $M$ with $K$ and a signature with message recovery (i.e., cleartext $M$ can be derived from $\{M\}_K$ under knowledge of the inverse key $K^{-1}$).

- $F$ represents any function in $\{\sigma, h, \text{enc}\}$

- $H$ is a one way function out of $\{\sigma, h\}$

- $\varphi$ and $\psi$ represents a formulae of the following kind:
  - $P \leftrightarrow Q$: $K$ is a shared key/secret between $P$ and $Q$.
  - $\text{fresh}(M)$: Message $M$ has been created in the current protocol run.
  - $M \equiv N$: $M$ is equivalent to $N$.
  - $P \text{ sees } M$: Agent $P$ was able to read $M$ as a submessage of a received message.
  - $P \text{ said } M$: Agent $P$ has sent the message $M$ and has been conscious of sending it at that time.
  - $P \text{ says } M$: Agent $P$ has sent the message $M$ knowingly and recently.
  - $P \text{ has } M$: $P$ knows message $M$ and can use it for further computations.
  - $P \text{ recognises } M$: Either $P$ has a reason to believe that $M$ is not a random string but willingly constructed or that $M$ is a random string already known to $P$.
  - $P \text{ controls } \varphi$: $P$ is able to decide whether $\varphi$ is correct or not.
  - $P \text{ believes } \varphi$: $P$ has strong evidence that $\varphi$ is correct.
  - $\neg \varphi$: Negation.
Appendix C. Rules of AUTLOG

- $\varphi \land \psi$: Conjunction.

Following are some of the rules of AUTLOG calculus that are used in the formal analysis of E2EUIC (the characters written in bold, preceding each of the rules (MP, K, J, H1, etc.) are the names of the rules as stated in [59]):

**MP:** If $\varphi$ and $(\varphi \rightarrow \psi)$ then $\psi$

**K:** $P$ believes $\varphi \land P$ believes$(\varphi \rightarrow \psi)$ $\rightarrow P$ believes $\psi$

**J:** $(P$ controls $\varphi \land P$ believes $\varphi)$ $\rightarrow \varphi$

**H1:** $P$ sees $X$ $\rightarrow P$ has $X$

**H2:** $P$ has $X_1 \land \ldots \land P$ has $X_n$ $\rightarrow P$ has $(X_1, \ldots, X_n)$

**H3:** $P$ has $X$ $\rightarrow P$ has $F(X)$

**F1:** fresh$X_1 \rightarrow$ fresh$((X_1, \ldots, X_n))$

**SE2:** $P$ sees enc$(K, X)$ $\land P$ has $K^{-1}$ $\rightarrow P$ sees $X$

**NV:** $P$ said $X$ $\rightarrow$ fresh$X$ $\rightarrow P$ says $X$

**A1:** $R$ sees $F(K, X) \land P \xrightarrow{K} Q \land \neg P$ said $F(K, X)$ $\rightarrow Q$ said $(K, X)$

**C:** $P$ sees $M \land M_P \equiv Y$ $\rightarrow P$ believes $P$ sees $Y$

**C1:** $P$ recognizes $X_i$ $\rightarrow (X_1, \ldots, X_n)_P \equiv ((X_1)_P, \ldots, (X_n)_P)$

**C3:** $P$ has $M$ $\rightarrow H(M)_P \equiv H(M_P)$

**E2:** $X \equiv Y \land Y \equiv Z$ $\rightarrow X \equiv Z$

**E3:** $X \equiv Y \rightarrow F(X) \equiv F(Y)$

**E4:** $X_1 \equiv Y_1 \land \ldots \land X_n \equiv Y_n$ $\rightarrow (X_1, \ldots, X_n) \equiv (Y_1, \ldots, Y_n)$

151