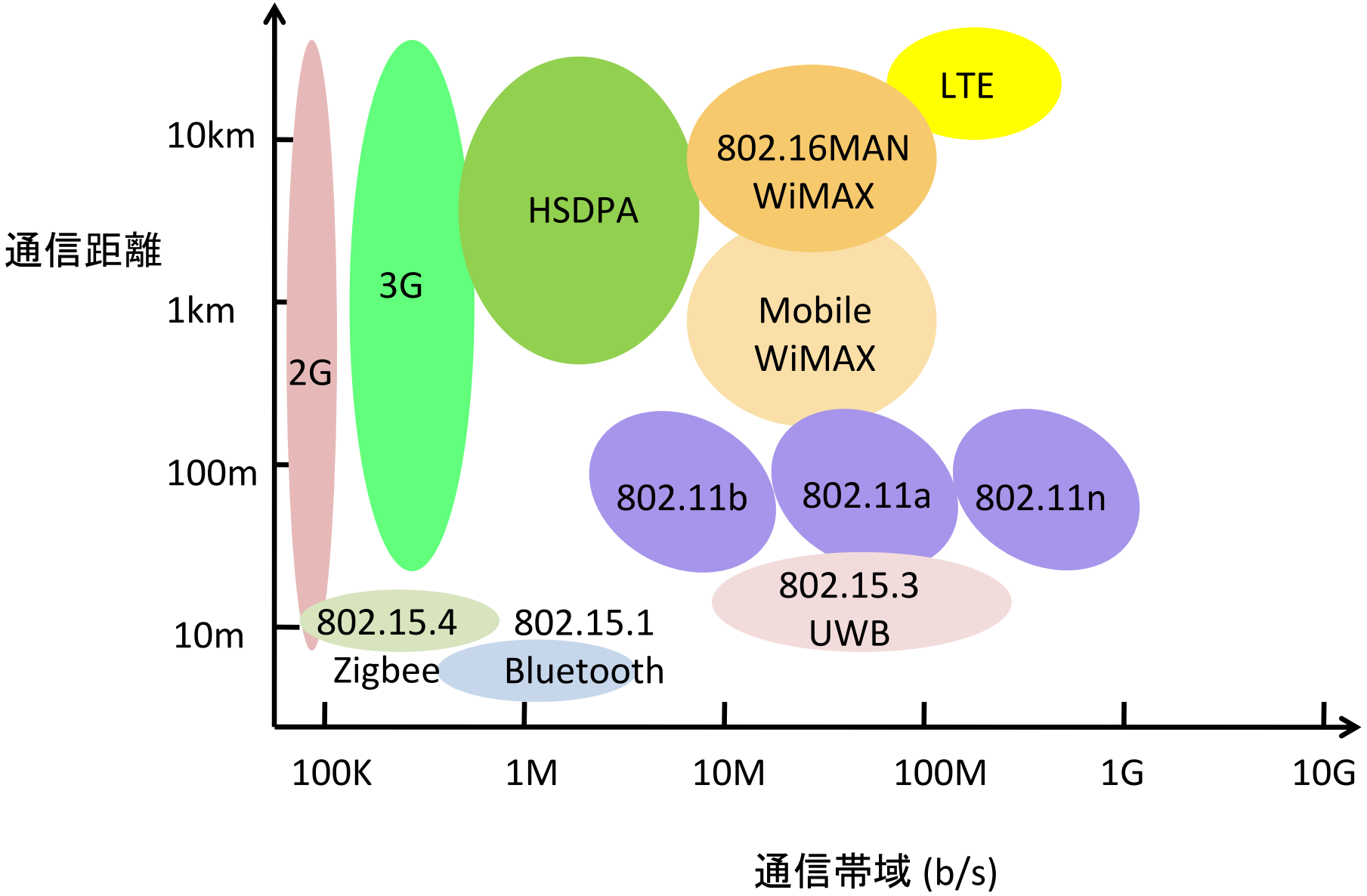
九州地域情報化研究会 in 佐賀

第四部　今後の地域情報化に向けて

ワイヤレスブロードバンドの技術動向

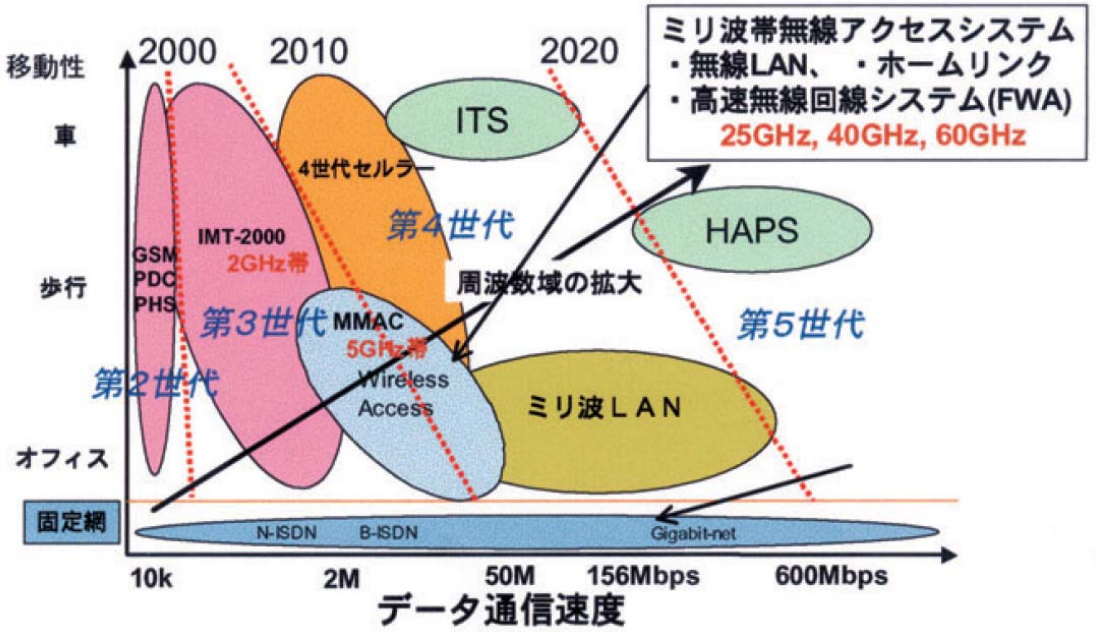
堀 良彰 〈hori@csce.kyushu-u.ac.jp〉
九州大学大学院
システム情報科学研究院

無線アクセスシステム


通信距離
10km
1km
100m
10m
2G
3G
HSDPA
LTE
802.16MAN
WiMAX
Mobile
WiMAX
802.11b
802.11a
802.11n
802.15.3
UWB
802.15.4
Zigbee
802.15.1
Bluetooth
100K
1M
10M
100M
1G
10G
通信帯域 (b/s)

ワイヤレスブロードバンドの要素技術（その1）

- デバイス関連技術
  - 半導体技術
    - GaAs系電子デバイス
      - GaAs FET, GaAS HEM
  - アンテナ作成技術
  - 無線用システムLSI
    - ディジタル信号処理技術



高周波デバイスの現状と将来市場（2002）
佐野芳明　佐野芳明沖電気工（株）より

ワイヤレスブロードバンドの要素技術（その2）

- 変調方式 (Modulation)：
  情報を伝送する際に最適な電気信号に変換する手法
- 複信方式 (Full Duplex)：
  双方向通信を実現する方式
- 多元接続方式 (Multiple Access)：
  複数の無線局に電波帯域を共有させる方式
- モビリティ確保技術 (Mobility)：
  無線局の移動を可能にする方式

ワイヤレスブロードバンドの要素技術（その3）

- ローミング・ハンドオーバ技術 (handover):
  異なるネットワークの切り替え
- セキュリティ技術 (Security):
  安全性確保や攻撃対策

変調方式 (Modulation)

- 周波数ホッピング・スペクトラム拡散（Frequency Hopping Spread Spectrum, FHSS）
  - 802.11
- 直接スペクトラム拡散（Direct Sequence Spread Spectrum, DSSS）
  - 802.11b
- 直交周波数分割多重 (Orthogonal Frequency Division Multiplexing, OFDM)
  - 802.11a/g, 802.16 WiMAX, 802.20 (MBWA), 802.16e, WiBro, 802.15.3a
- 広帯域通信 (Ultra Wide Band, UWB)
  - 802.15.3

（サブ）キャリア変調方式

- BPSK･･･2相位相変調
- QPSK ･･･ 4相位相変調
- 16QAM ･･･ 16値直交振幅変調
- 64QAM ･･･64値直交振幅変調

複信方式 (Full Duplex)

- 時分割複信 (Time Division Duplex, TDD):
  情報を時間軸で圧縮し、送受信方向を切替え

- 周波数分割複信 (Frequency Division Duplex, FDD):
  周波数帯域を分割する

多元接続方式 (Multiple Access)

- 符号分割多元接続 (Code Division Multiple Access, CDMA)：拡散符号を利用するスペクトル拡散変調
- 時分割多元接続 (Time Division Multiple Access, TDMA)：固定タイムスロット割当によるアクセス
  - 802.20 (iBURST)
- 周波数分割多元接続 (Frequency Division Multiple Access, FDMA)：周波数帯域を分割し割当
  - OFDMA：OFDM を利用した多重アクセス方式
    - 802.15e Mobile WiMAX
- 空間分割多元接続 (Space Division Multiple Access, SDMA)：複数アンテナを利用した空間的多重アクセス方式
  - MIMO (Multiple Input Multiple Output)
    - 802.20 , 802.11n

多元接続方式 (Multiple Access)

- キャリアセンス多重接続 (Carrier Sense Multiple Access, CSMA) :（帯域の）空きを見ながら間欠送信
  - CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
    - 802.11系, ZigBee, UWB

モビリティ確保技術 (Mobility)

- モビリティのためのルーティング技術
  - MIP(v4), MIPv6
- ハンドオーバー機能
  - 同じネットワーク内でのハンドオーバ
  - 異種ネットワーク間のハンドオーバ
    - IEEE 802.21
      - WiFi と WiMAX 間など異種プロトコル間のハンドオーバ等を実現
    - 4G といっているもの
- ローミング技術
  - 携帯電話網GSM, WCDMA
  - IEEE 802.11r

セキュリティ技術 (Security)

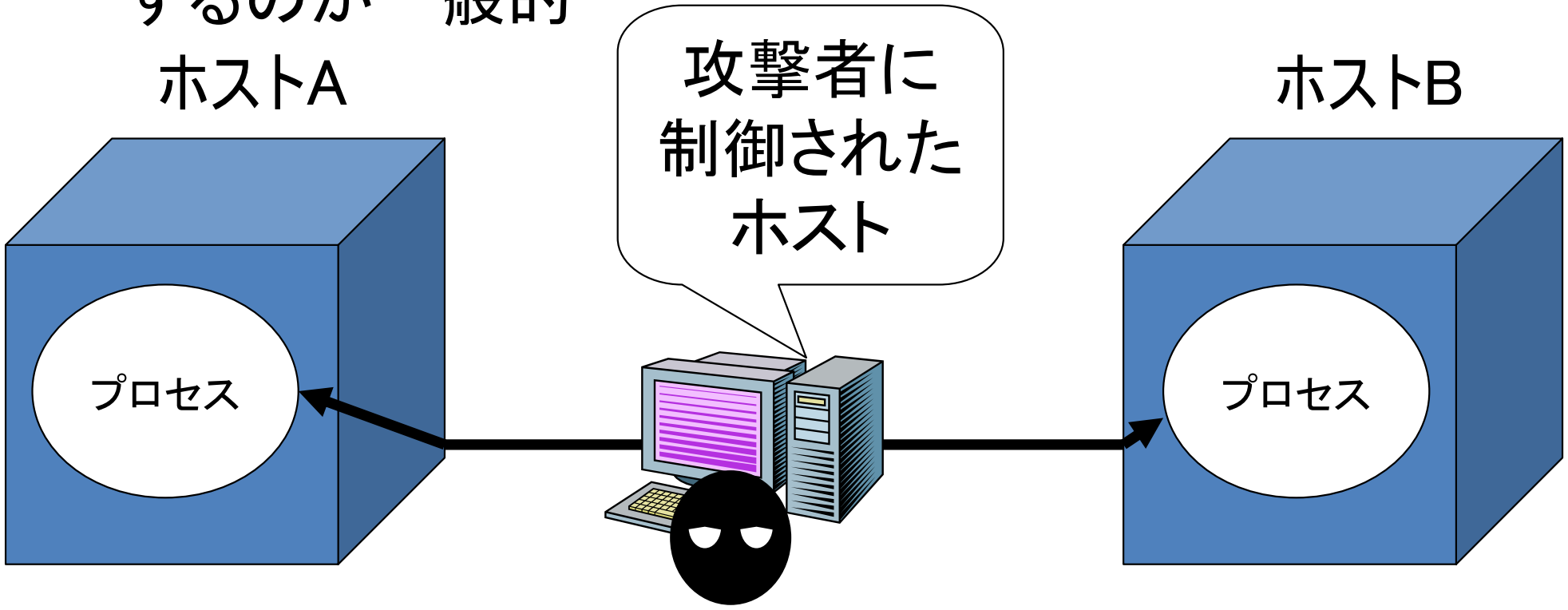
- WEP (Wired Equivalent Privacy)
  - IEEE 802.11
- WPA (Wireless Protected Access), WPA2
  - IEEE 802.11+WPA, IEEE 802.11i
- PKM (Privacy Key Management)
  - IEEE 802.16 WiMAX, IEEE 802.16e Mobile WiMAX

脅威 (threat)

- ネットワークの信頼性や安全性に対する脅威(threat)は多種多様
- ネットワークの構成要素
  - ネットワーク機器・・・ネットワークを構成する
  - ネットワークに接続されるコンピュータシステム・・・サービスを提供・利用
- どのようなセキュリティ技術が必要になるかという議論のためには構成要素に対する脅威を明らかにする必要がある
  - ネットワークそのものに対する脅威
  - ネットワークに接続されるシステムに対する脅威

ネットワークシステムで想定する脅威

- ネットワークそのものに対する脅威を考える場合、通信をする二つのプロセスの間に、悪意を持ったユーザによって完全に制御されている状況を想定するのが一般的



無線ネットワークでは？

- 物理的保護に頼れない
- シグナル伝達はブロードキャスト
- その結果
  - 盗聴容易
  - メッセージの挿入容易
  - 再送（攻撃）容易
  - 不正アクセス容易
  - DoS (Denial of Service) 攻撃容易

ネットワークシステムで想定する脅威

- 先に述べた状況・・・二つのプロセス間に通信路で想定可能な攻撃（attack）としては次のものが挙げられる
  - 盗聴（eavesdropping）
  - トラヒック解析（traffic analysis）
  - 通信路改変（stream modification）
  - 通信不能攻撃（denial of service）
  - なりすまし（masquerading）
  - その他

無線セキュリティ対策の目的

- 次の項目に対する確保が必要
  - 秘匿・認証・完全性チェック・再送（攻撃）検出・アクセス制御・ジャミング攻撃からの保護
- 何に関して？
  - データグラム中継、名前・アドレス、隣接ノード発見、接続確立、ルーティング、

対策技術

- 暗号アルゴリズム
- （暗号）プロトコル
  - 鍵共有・鍵生成
  - 認証
- etc.

無線LANのセキュリティ

無線LANのセキュリティ項目

- 通信している内容を第三者に知られないようにする秘匿（暗号）技術
- 通信の相手が正しい相手かどうかを確認する認証技術
- 暗号や認証のための鍵管理（鍵配送）技術
- 第三者が偽のデータを送った場合にそれを検出する改ざん検出技術

無線LANのセキュリティ機能

（従来のもので利用できる）

- WEP (Wired Equivalent Privacy)
  - 共有鍵方式を用いた認証、暗号化
- MACアドレスフィルタリング
  - アクセスポイントに登録されたMACアドレスしか通信できない
- SSID (ESSID)
  - アクセスポイントのESSIDを知っている人だけが通信できる

（新しいもので利用できる）

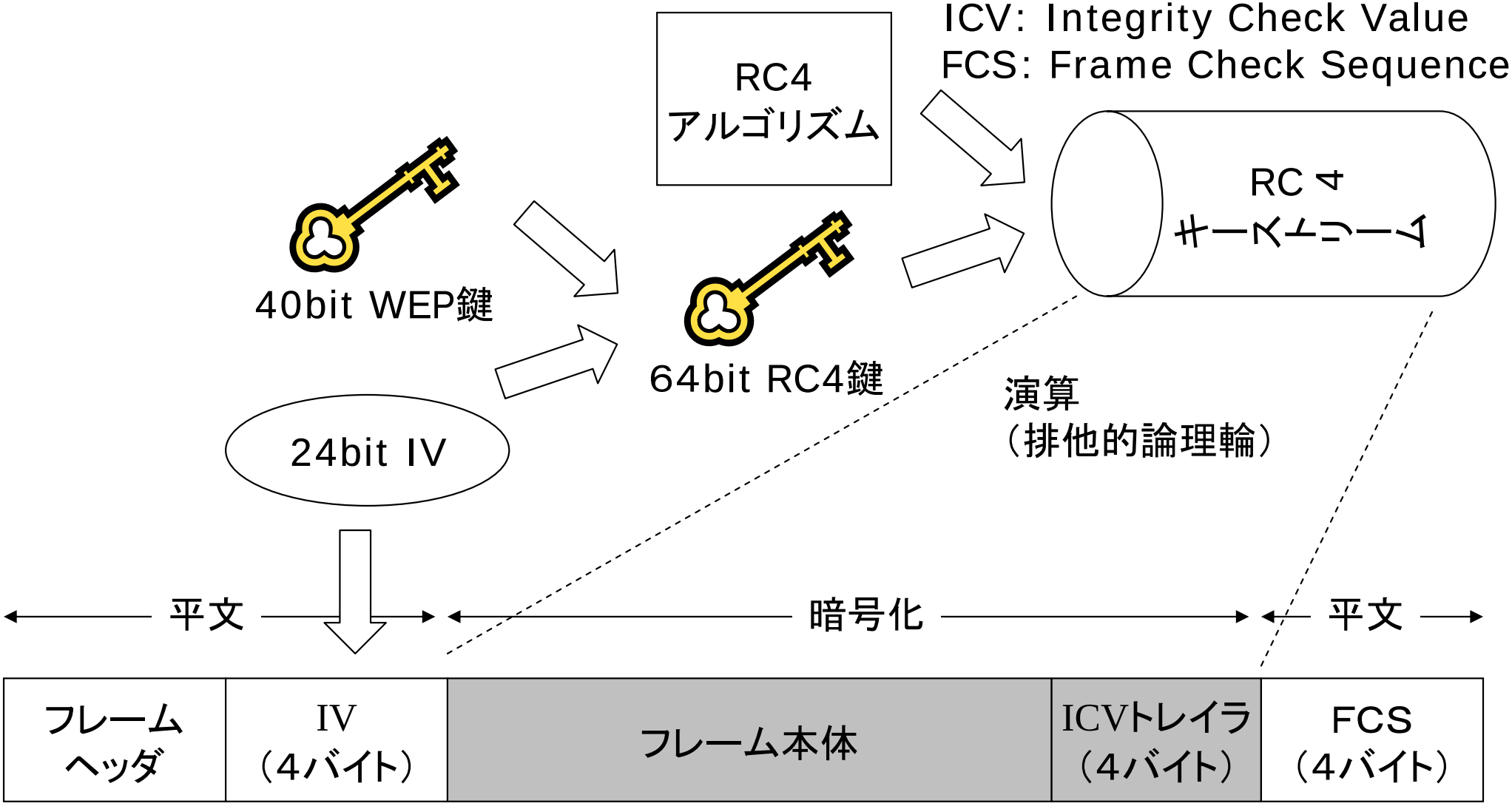
- 802.1X認証
  - ユーザ認証と個別の暗号鍵配布
- WPA
  - 802.1X, TKIP などの組み合わせにより、ユーザ認証を行いWEPの弱点をカバー
- IEEE802.11i (WPA2)
  - 新たな暗号化方式 AES の使用

WEPによる暗号化

- データを保護（暗号化）するために、WEPでは対称性を持つストリーム暗号RC4を使用する
  - ストリーム暗号・・・キーストリームと呼ばれるビット列とメッセージの演算により暗号文を生成する。受信者は同一のキーストリームを用いて復号する
  - キーストリームの生成・・・多くのストリーム暗号では比較的短い秘密鍵を用いて、対象のメッセージと同じ長さの擬似乱数キーストリームを生成（送信者、受信者とも）
  - ストリーム暗号のセキュリティは、キーストリームのランダム性に依存

WEPの操作

RC4: Rivest Cipher 4
IV: Initialization Vector
ICV: Integrity Check Value
FCS: Frame Check Sequence



フレーム構成

WEPの脆弱性

- 当初から、設定キーが40bitと短いことなどから、安全性が懸念されていた
- 2001年夏、ShamirらによりWEPの解読について発表
- RC4 では同じ暗号鍵を使用したデータを収集して解析すると、暗号化される前のデータを推測しやすくなる
- 固定の事前共有鍵とIVで鍵を生成するが、IVの空間が24ビットと短い。また特定のIVにおいては、より解析が容易になる
- WEP解読ツール AirSnortのリリース

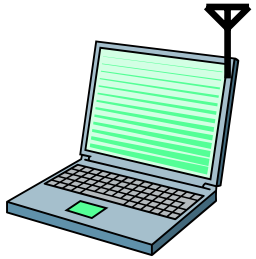
グループ共通鍵の問題

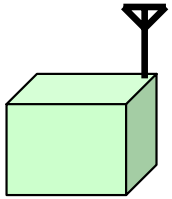
- 同じ暗号鍵を継続して使用すると、時間の経過とともにセキュリティは低下する
- グループのメンバが入れ替わったときに、新たな鍵を配布する？
- 一つのアクセスポイント(ESS)について、一つの認証鍵を多くの端末で共有しなければならない
  → 鍵が漏れる可能性高
  → 秘密は大勢で共有してはいけない

無線LAN(802.11)における認証

- 共有鍵認証方式
  - 暗号化用の鍵と同一の鍵を使用
  - チャレンジーレスポンス方式
    - A: 乱数を発生z
    - A→B: 乱数を送る
    - B→A、共有鍵で乱数を暗号化したもの
    - A: 乱数を共有鍵で暗号化したものと比較
  - 通信を行う二者（アクセスポイント、ステーション）は、あらかじめ鍵を共有させておく
- オープン認証方式
  - すべての認証要求を許可・・・認証を行わないのと同じ

認証の手順（共有鍵認証）





クライアント　　アクセスポイント

プローブ要求 →

← プローブ応答

認証要求 →

← 認証応答 with チャレンジ

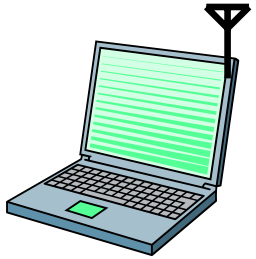
認証応答 with レスポンス →

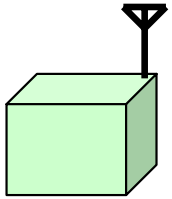
← 認証応答（成功）

アソシエーション要求 →

← アソシエーション応答

認証の手順(オープン認証)





クライアント　　アクセスポイント

プローブ要求 →

← プローブ応答

認証要求 →

← 認証応答(成功)

アソシエーション要求 →

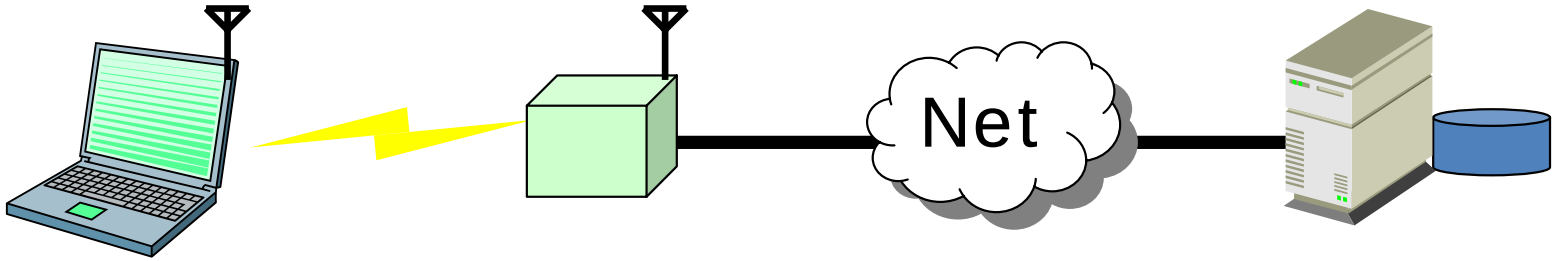
← アソシエーション応答

WEP認証プロトコルへの攻撃

- 認証はチャレンジレスポンスプロトコルが利用される
  - AP → STA: r
  - STA →AP: IV | r XOR K
    - ここで、K は IV と共有秘密鍵から導出される 128bit RC4 の出力
- 攻撃者の準備
  - r XOR (r XOR K) = K を計算可能
- 攻撃
  - AP → attacker: r’
  - attacker → AP: IV | r’ XOR K

IEEE802.1Xを用いた認証と鍵配送

- 本来は、LANスイッチなどネットワーク機器のポート単位でのユーザ認証を実現するもの
- 認証成功してはじめて、アクセスポイントはクライアントをNetに接続
- どのアクセスポイントからも参照できる認証情報データベースを用意
- WEP暗号鍵をクライアントに配布・更新することができる



クライアント

アクセスポイント

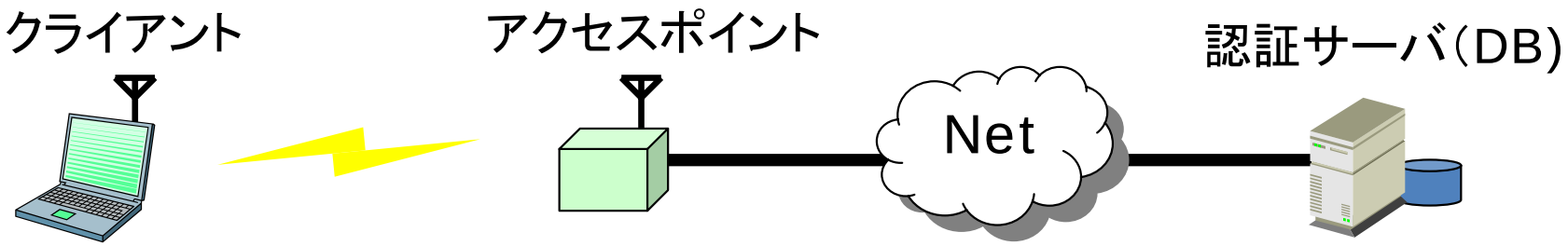
認証サーバ（DB）

（802.1X用語） (Supplicant)

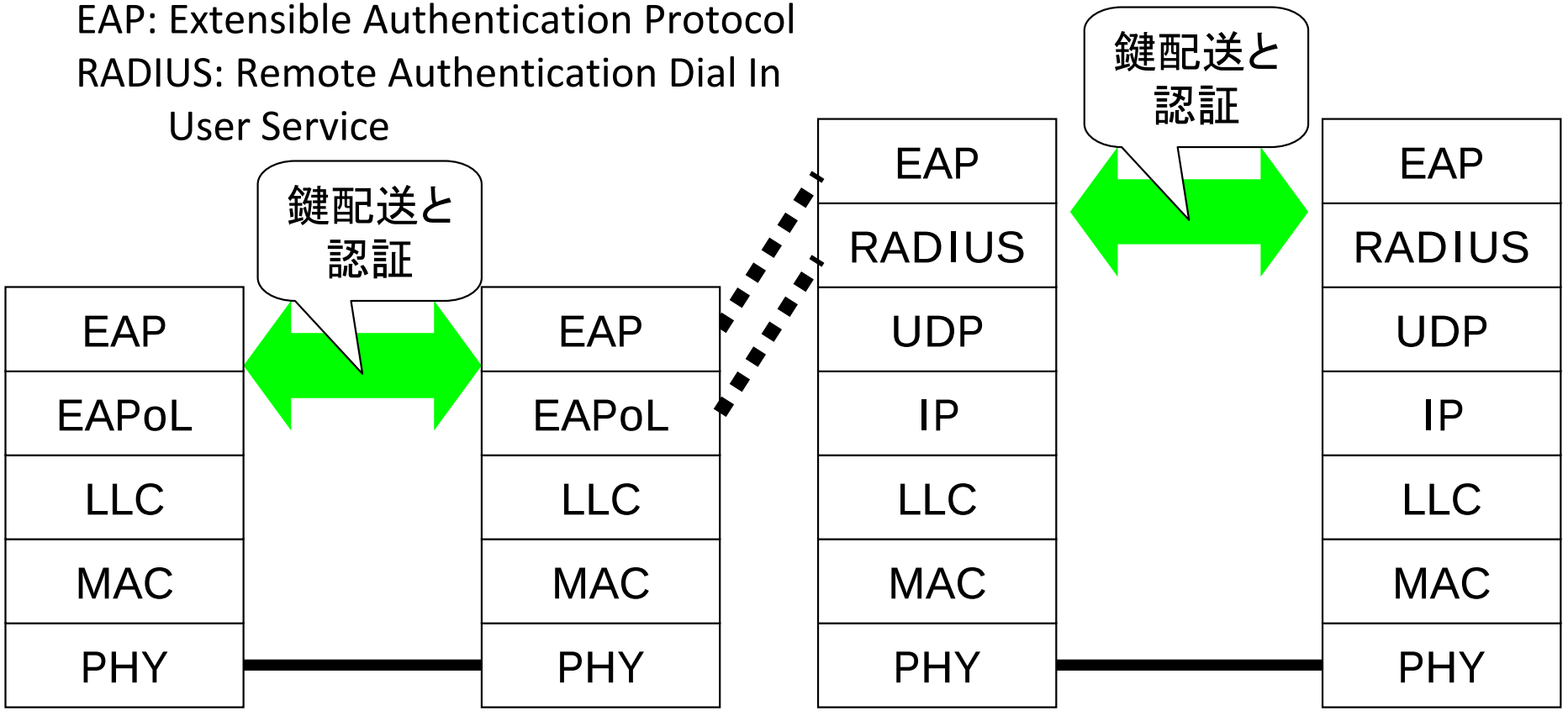
(Authenticator)

(Authentication Server)

802.1Xのプロトコルスタック



EAP: Extensible Authentication Protocol
RADIUS: Remote Authentication Dial In User Service



EAPのフレームワーク上で用いられる認証プロトコル

- EAP-TLS
  - EAPフォーマットのパケットで、TLSプロトコルを用いる
  - パスワードを使用せず、公開鍵認証を使用する
  - 公開鍵証明書を証明するためのCAも必要
- EAP-TTLS, EAP-PEAP
  - パスワードを使用した認証方式
  - ユーザはサーバから配送された公開鍵を用いて、パスワードを暗号化して送る
  - サーバは秘密鍵でパスワードを復号し検証する

WPA (Wi-Fi Protected Access)

- WEPの弱点を補強する規格として Wi-Fi AllianceはWPAを規定した
- WPAは複数のセキュリティ規格の総称
  - ユーザ認証を行う IEEE 802.1X
  - 新しい暗号化方式である TKIP
- WPAの２つのモード
  - WPA-EAP (Extensible Authentication Protocol)
  - WPA-PSK (Pre-Shared Key)

WPA-EAP と WPA-PSK

	EAPモード	PSKモード
対象	企業または公衆無線LAN事業者	SOHOおよび一般家庭
RADIUSサーバ	必要	不要
暗号鍵生成	TKIP(RC4)	TKIP(RC4)
暗号鍵生成(option)	AES	AES
認証	IEEE 802.1X	Pre-Shared Key

TKIP (Temporal Key Integrity Protocol)

- WEPの枠組みを変えずによりセキュアにする
- WEPの欠点
  - パケットを容易に偽造可能
  - リプレイ攻撃ができる
  - IVの値から弱いものを見つけることができる
  - 同じIVと同じ共有鍵を使って暗号化されることが多い
- TKIPでの改良点
  - ハッシュ値に相当するMIC(Message Integrity Code)の導入
  - IVをカウンタとして利用し、受信済みのIVより小さいIVを含むパケットを受け取らない
  - IVとWEPキーをシャッフルしてキーストリーム発生の種を推測できないようにする
  - IVを48ビットに拡張子、重複しないようにする。ユーザ毎に異なる鍵で暗号化する

WPA2

- WEP → WPA → WPA2
  - WEPより2世代先
- WPA2は、IEEE802.11iに準拠
- WPA2(IEEE802.11i)は、National Institute of Standards and Technology (NIST; 米国標準技術局) FIPS 140-2 に準拠するAESを採用
- WPA2はWPA下位互換
- WPAとWPA2の相違点は、暗号化方式。RC4とAES

WPA and WPA2

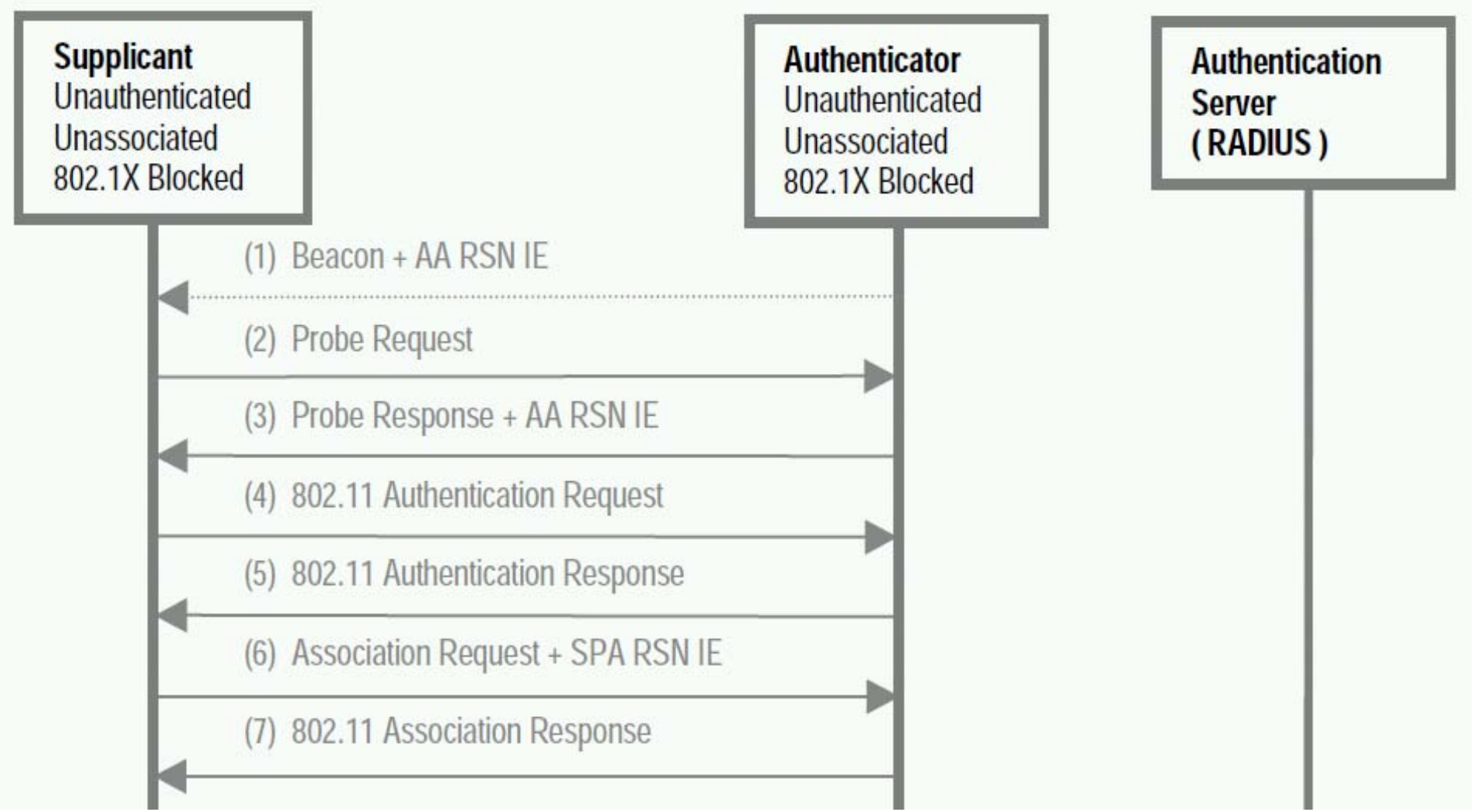
From Wi-Fi is everywhere!
Wi-Fi Protected Access Web Cast,
Wi-Fi Alliance, June 2003

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

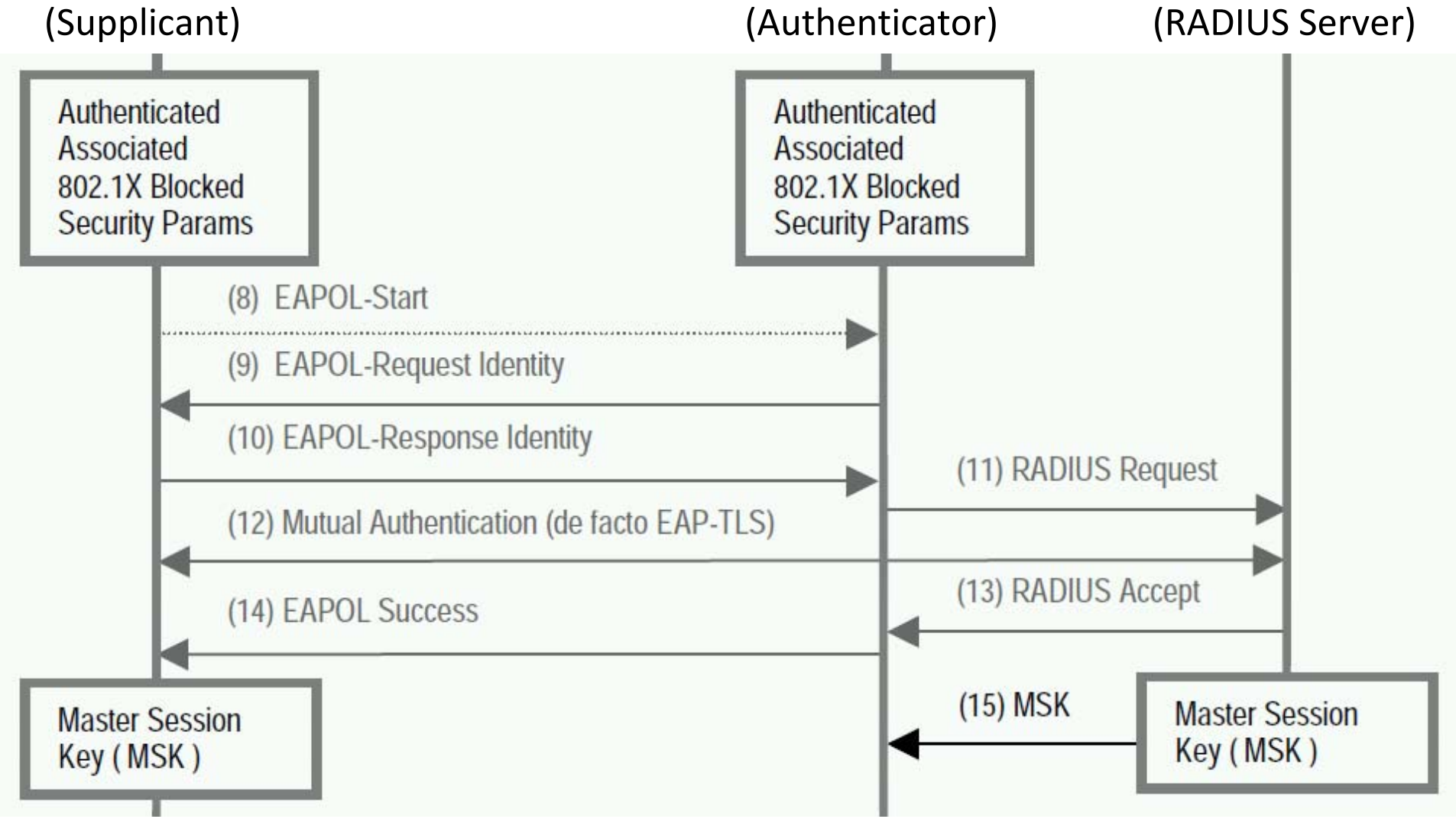
IEEE 802.11i 概要

- 2004年6月に標準化
- データ秘匿、完全性チェック、相互認証を提供
  - 3つのデータ秘匿プロトコルを提供
    - Temporary Key Integrity Protocol (TKIP)
    - Counter-mode/CBC-MAC Protocol (CCMP) with AES-128 (128bit Key and 128bit Block size)
  - 認証および鍵管理プロトコル
    - Extensible Authentication Protocol (EAP)のサポート
      - EAP-TLS など EAPの枠組みを用いた認証プロトコルが利用可能
    - 4ウェイハンドシェイクを用いて共有メイン鍵から、一時共有鍵を生成
  - 従来の802.11 WEP のサポート

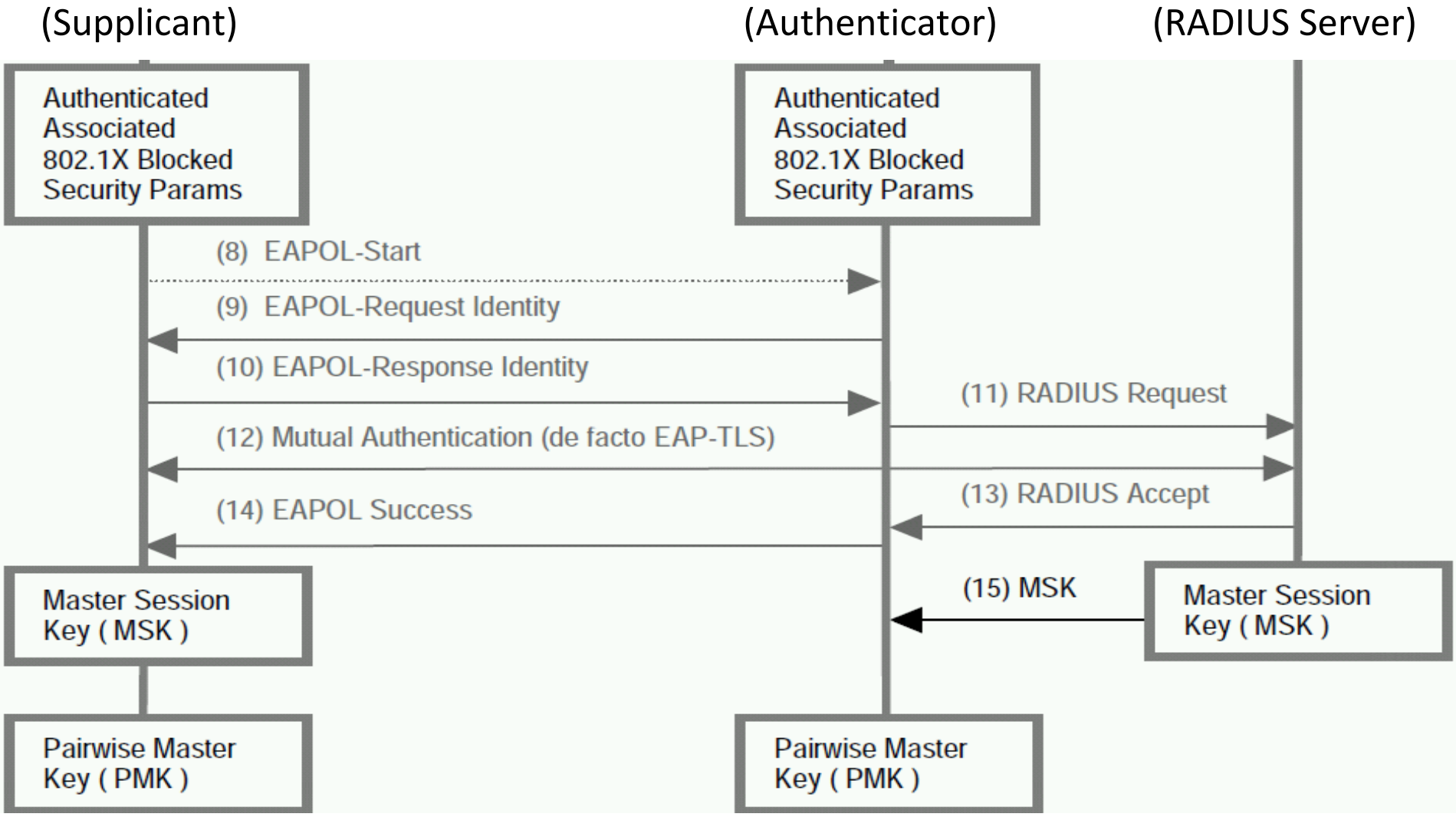
802.11i RSNA time line (1st stage)



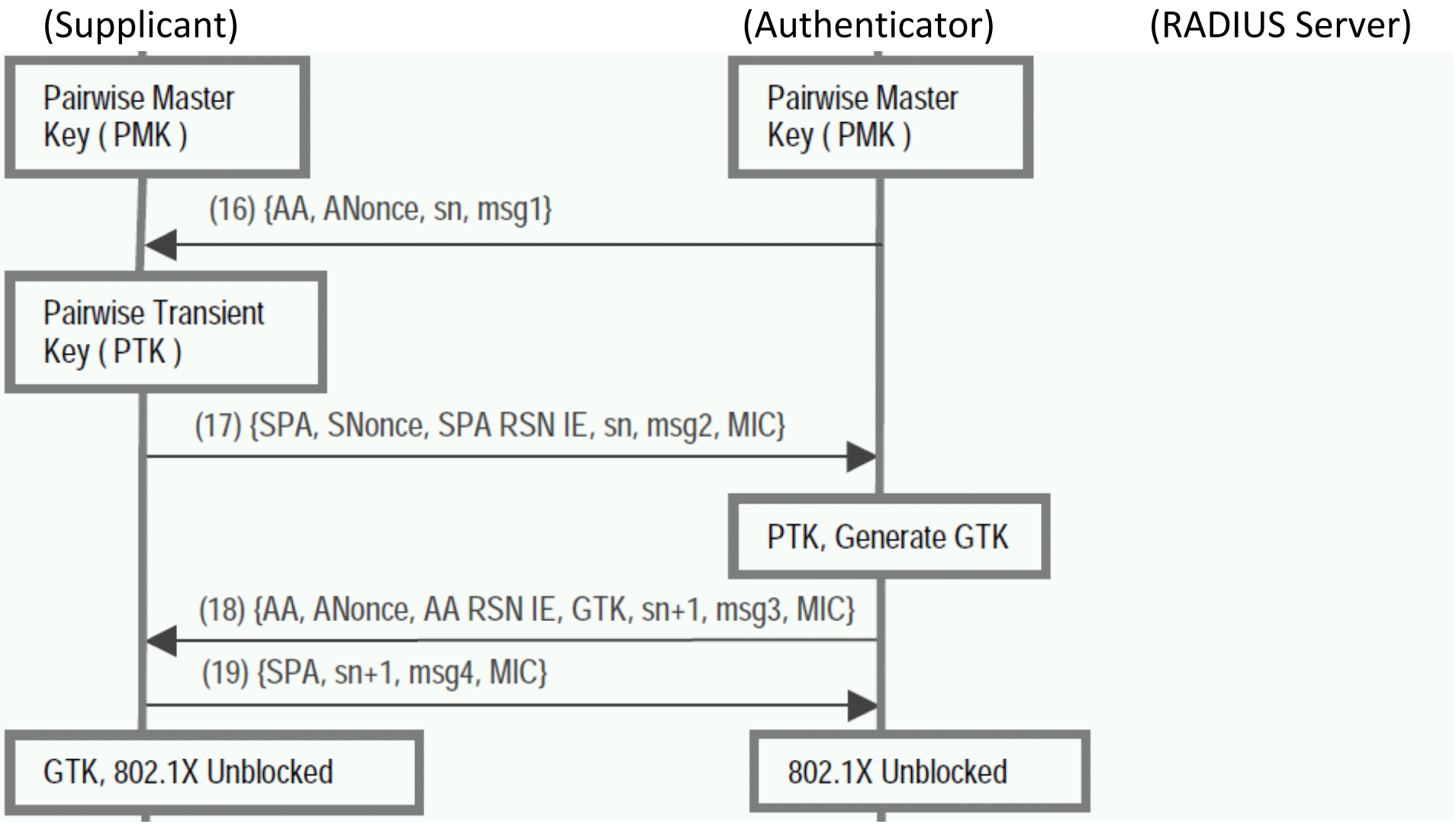
802.11i RSNA time line (2nd stage)



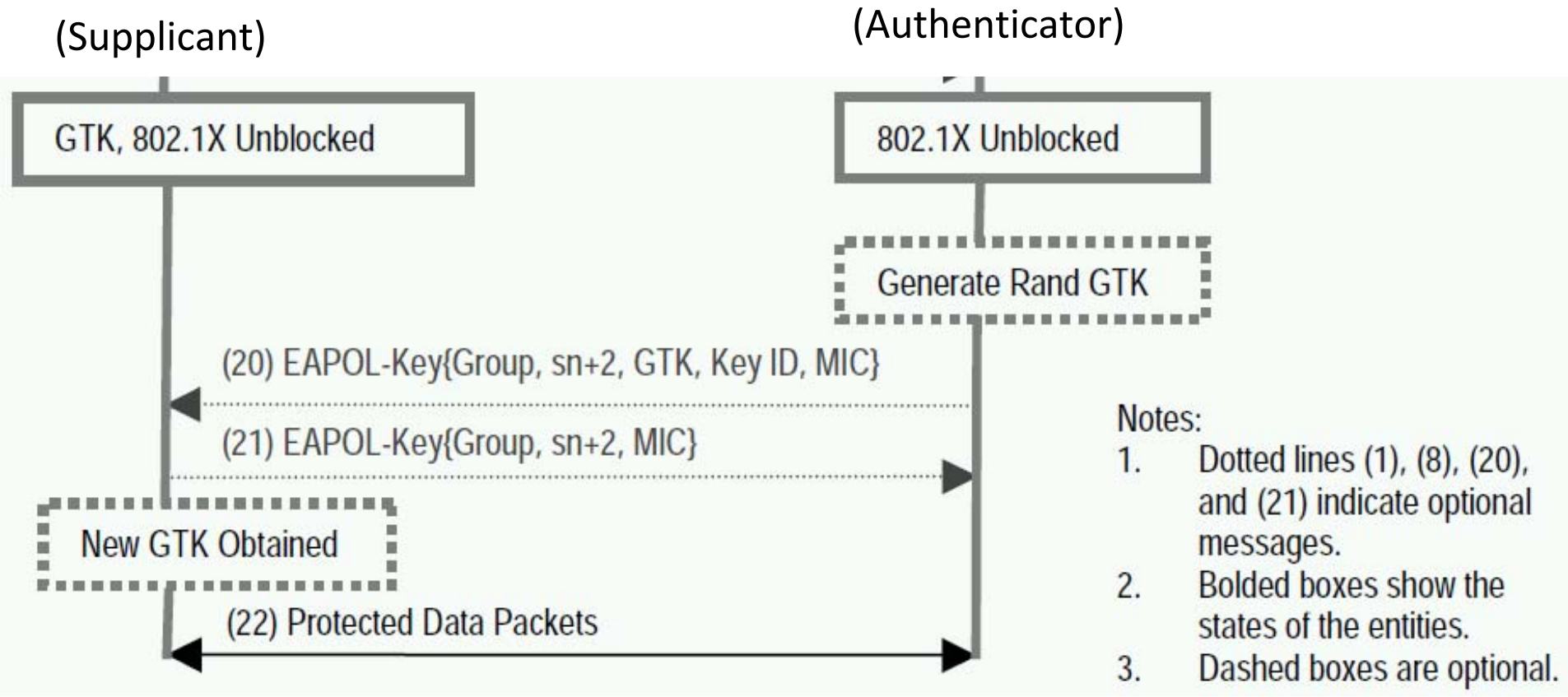
802.11i RSNA time line (3rd stage)



802.11i RSNA time line (4^{th} stage)



802.11i RSNA time line (5th stage)



残された問題 DoS 攻撃

- 攻撃者が管理フレームを偽造しての攻撃
  - 802.11i の枠組みでも、制御フレームの認証は不能
    - 認証終了(Deauthentication)フレームやアソシエーション終了(Deassociation)フレームを偽造
- 対応
  - 管理フレームの保護 → 802.11w WG
    - March 2009 の標準化を目指す
    - 管理フレームの重要性が高まる
      - 11k 計測拡張
      - 11r ローミング拡張
      - …..

WiMAX セキュリティ

- IEEE 802.16-2004 WiMAX セキュリティ: PKM(v1) (Privacy and Key Management)
  - 認証: RSAベースの一方向認証（のみ）
  - 暗号: 3DES, RSA, AES（鍵）、DES, AES（データ）
- IEEE 802.16e Mobile WiMAXセキュリティ: PKMv2
  - 認証: EAP・RSAベースの双方向認証
  - 暗号: AES（鍵）、DES, AES（データ）
  - ハンドオフ時の事前認証

難しさ

- 確立されたセキュリティ要素技術を使っても、セキュアなシステムを構築できるとは限らない
- システムとしての安全性評価が必要
- 評価手法
  - 形式的手法 (formal method)
    - 安全性を論理的に導出
      - 推論規則による方法
      - システムが取り得るすべての状態について検証する方法

新しいワイヤレスアーキテクチャ

- メッシュネットワーク Mesh Network
  - 多数の中継ノードが協調して、バックボーンインフラを形成 → 自己組織的形成機能が不可欠
    - 信頼はどこに？
    - ノードの利己性(selfishness)をどう排除するか
      - 中継しない
      - 共用資源の使いすぎ
- 車対車間通信 Vehicular Communication
  - 信頼はどこに？
  - 可用性確保
    - DoS 対策 incl. jamming

まとめ

- 要素技術は、確立されている
- システム化技術は、まだまだこれから
- 市場にあらわれた技術に関して考察が必要
  - 何がどこまでできるのか
  - 何ができないのか
  - 近いうちに何ができるようになるのか