Security of Wireless Networks

Summary Andreas Biri, D-ITET 06.01.18

1. Introduction

Infrastructure-based:

- *Cellular:*	DATA
- *WiFi:*	DATA
- *GPS:*	LOCATION, TIME
- *Indoor Localization:*	LOCATION
- *RFID tags:*	IDENTITY

1.1 Basics: Security Notions

Confidentiality: encryption should prevent attacker to learn anything in addition to what he already knows

Semantic security: learn nothing about *plain*text from *cipher*text (know same as before looking at it)
- requires randomization; same plaintext should always result in different ciphertext

Authentication: everyone can verify origin of message

Symmetric Key Cryptography

Stream ciphers: plaintext XOR-ed with output of stream
- RC4: very simple design

Block ciphers: operate on blocks of data
- AES (*Advanced Encryption Standard*)

Message Authentication Codes (MACs)

MAC function takes msg & secret (symmetric) key and outputs an authenticator of a fixed length ("a MAC")

Only achieves authentication / integrity
- for confidentiality, add encryption as an outer layer

Asymmetric (Public) Key Cryptography

Confidentiality: encrypt with P_{public}, decrypt with $P_{private}$

Authentication: encrypt with $P_{private}$, decrypt with P_{public}
- Signature: compute over the hash of the message

1.1 Basics: Wireless Communication Systems

Attacks

Jamming: "blind" the system, obvious to everyone

Spoofing: force errors/misclassifications without anyone realizing, e.g. by adding artificial antennas
- alter content of message (violate integrity)
- forge new / replay packets without anyone realising

Selection: "To whom should I send all / part of it?"

Waves & Frequency

Baseband: signal containing only information

Carrier: pure sinusoid of particular frequency & phase

Modulated signal: carrier modulated with information

Amplitude Shift Keying (ASK): Switch amplitude depending on signal which should be transmitted

Frequency Shift Keying (FSK): switch frequency

Phase Shift Keying (PSK): switch phase between bits

Required bandwidth depends on modulation techniques

Antenna

Key properties: transmitted power, carrier frequency, bandwidth, modulation type

Phased array: steer array to transmit signals from specific direction by adjusting phase of antenna accordingly so that all in phase when viewed from a certain direction

2. Physical Layer / Jamming

2.1 Jamming

Preventing or reducing ability of communicating parties to pass information by deliberate use of EM signals
- Unintentional interference: mostly Gaussian
- Intentional interference: Rx can no longer decode

Jam-proofing: force attacker to transmit with high power
- reveals the attacker, i.e. location and/or identity

Symbol jamming: corrupt symbols aren't decoded correctly
Communication jamming: prevent despite Error Correction

Try to transmit on the right frequency with approximately the same power as the original signal to succeed
- in order to find frequency, mostly need to send broad-band signals which cost a *lot* of energy for the attacker

Burn-through range: range at which the sender succeeds in communicating with the receiver *despite* jamming

2.2 Jamming Resistency

If you cannot fight, *RUN and HIDE*

Need advantage over the attacker: *shared secret*

Frequency Hopping Spread Spectrum (FHSS)

Derive pseudorandom hopping sequence derived from key
- requires *synchronization*, e.g. using GPS in advance

FHSS Partial Band Jammer: Jammer has to jam all possible frequencies and therefore has to distribute its available power over the spectrum so that ≅ power of signal

FHSS Follower Jammer: *search & destroy* signal in realtime
- need to be fast enough to switch before jamming starts

Detectability: FHSS transmitter do not really hide
- can be found using *Angle-of-Arrival* detection
- original signal still clearly visible for anyone

Direct Sequence Spreading Spectrum (DSSS)

Spread the signal and *"hide in noise"* **(need noise!)**

Use **CDMA** to spread Narrowband waveform below noise level, so that only the correct (same) **spreading code** can again decipher the original message (2x same algorithm)
- *Wide*band jammer: XOR preserves randomness → spread (still possible however with enough power available)
- *Narrow*band jammer: spread instead of despread

Spread by XORing baseband with a high-frequency code
- can send with **very low power, as high redundancy** by sending many chips for the same bit of information

Processing gain: ratio of chip rate to information bit rate

Can be applied to:
- send information despite low energy reception, as high redundancy and reception over long time
- receive despite interference, intentional by attacker or unintentional by environment / other spreading codes
- hide sender in the noise and make him invisible

Codes need to have good auto- and cross correlation properties (pseudorandom rather good / orthogonal)
- low *cross*-correlation (CDMA) to separate channels
- low *auto*-correlation to eliminate multi-path interference

Detection still possible due to:
- energy detection (targeted antenna with AoA)
- signal characteristic (constant chip rate)

LPI: *low probability of interception*

Chirp

Use frequency sweeping to send signal over entire spectrum available to decrease probability of intercept

3. GNSS (GPS) Security

GNSS: Global Navigation Satellite System
- 24 satellites at 20'200km above earth
- message includes *location & precise time of transmission*

Spreading codes

- Trade-off between rate & robustness (use less power)
- Used to differentiate satellites with CDMA

Coarse: 1023 chips transmitted at 1.023 Mbits
- 20'000 chips/bit (50bps), 1 chip / μs

Precision: $6.1871 * 10^{12}$ chips, repeated once a weak
- allows more precise timing (100ns) and 10^{-18} Watt Rx

Time of Arrival: find high correlation by shifting through
- use two registers for *Coarse* and *Precision* mode

Doppler shift: search $\pm 50\ Hz$ due to movement of Tx/Rx

Find position by solving 4 equations (one for each sat) using Taylor series linearization & finding p & τ (clock error)
- determined by **difference in time-of-arrival** (as Rx might by out of sync, sats are assumed to be perfectly in sync)

3.1 Spoofing attacks

Modify content: spoof resulting position
(not possible in military GPS signals, as authenticated)
Modify arrival time (delay): spoof resulting clock on device

No authentication for civilian navigation messages

3.2 Countermeasures

Cryptographic authentication: military applications where it is practical to distribute keys, GALILEO sells them

Signal characteristics:
- Direction of arrival, phase measurements
- received signal strength, AGC (*Automatic Gain Control*)
- Additional sensors to validate position / velocity / time

Direction of arrival: hard due to multipath propagation
- use multiple antenna with known distance in-between

Signal strength: spoofed signals lead to valid signal being categorized as noise, can be seen in noise variation of AGC

SPREE: Auxiliary Peak Tracking using a *single receiver*
- attacker slowly increases his signal to bait receiver into locking onto his signal instead of the valid one
- SPREE tracks multiple peaks to detect seamless takeovers
- "Is this spoofing or multipath?" → categorize as spoofing if $> 100ns$, as unrealistically large multipath (does not reliably work for small spoofs, as indecisive)

Leveraging Spatial Diversity: using multiple receivers
- measure simultaneously with known constellation of receivers which do not change position
- assume attacker only has a single antenna for all signals
- received signal only delayed for different receivers
  → calculate same position which we know is not possible

Broadcast systems can never be fully secure

(assuming Dolev-Yao attacker)

Require either:
- bidirectional communication
- communication from the device to the infrastructure

Can use **TESLA** to create cryptographically secure packets
- cannot be forged if device can read broadcasts
- not possible to prevent replay attacks of entire stream

4. Secure Localization

Previously, relied on reduced communication range
- Inductive coupling
- Radio communication

4.1 Secure Proximity Verification

Measured distance should be an *upper bound* on the true distance between verifier and prover
- attacker can always delay, but that does not improve it
- maximally cheat for 1-2ns (15-30cm) on prover side

Early detect: "As soon as can reliably detect, I answer"
- results in earlier response, "shorter" distance
- predict bit even before completely receiving it

Late commit: leverage receiver tolerance/robustness
- attacker sends garbage, commits as soon as realizes actual signal so that "start" of response is earlier

Symbols should therefore be *as short as possible*
- difficult due to spreading with distance, noise

In order to prevent prover from cheating, he should not be executing any demodulation / extensive function

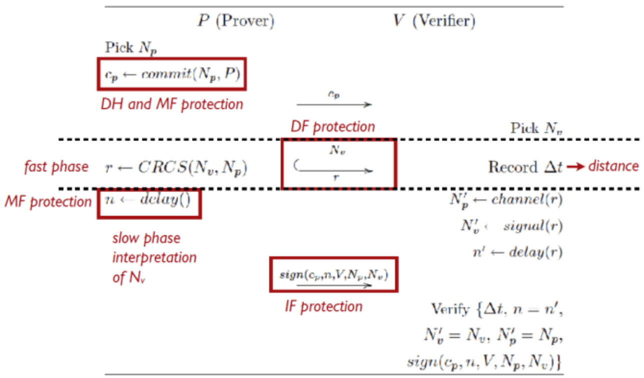
CRCS: *Challenge Reflection with Channel Selection*

→ Prover does not interpret N_V, but only **reflects** challenge
- depending on challenge, select correct channel to return
- Verifier has to check whether challenge returned correctly (stich together both channels to see result)

Distance fraud: dishonest prover wants to appear nearer

Mafia fraud: attacker convinces honest parties that near

CRCS protects against both:
- *DF*: time-critical phase which needs to be executed fast
- *MF*: force to commit first so we know where prover will answer (N_P) & prevent "too long computation time" (n)



P (Prover)
V (Verifier)
Pick N_p
$c_p \leftarrow commit(N_p, P)$
DH and MF protection
c_p
DF protection
Pick N_v
fast phase
$r \leftarrow CRCS(N_v, N_p)$
N_v
r
Record Δt → distance
MF protection
$n \leftarrow delay()$
$N_p' \leftarrow channel(r)$
$N_v' \leftarrow signal(r)$
$n' \leftarrow delay(r)$
slow phase interpretation of N_v
$sign(c_p, n, V, N_p, N_v)$
IF protection
Verify $\{\Delta t, n = n', N_v' = N_v, N_p' = N_p, sign(c_p, n, V, N_p, N_v)\}$

DH: *Distance Hijacking* (claim I just answered correctly)

IF: *Impersonation Fraud* (say I'm someone else)

1. *Commitment:* prevent sending response before challenge
2. *Rapid bit exchange*: send challenge & response
3. *Final verification:* check if responses are from prover

4.2 Verifiable Multilateration

Distance enlargement: always possible by delaying signal

Distance reduction: not possible if relying on speed of light

Secure localization: compute correct location of (trusted) device in the presence of an attacker

Location Verification: verify location of untrusted device

Bidirectional communication allows asynchronous clocks, as round-trip does not depend on clock drift

Verifiers (known locations) form a *verification triangle*
1. *P* cannot successfully claim false location inside
2. *M* cannot convince anyone of false location inside
3. Anyone can spoof outside of the triangle

Attacks

- MMSE estimator can be tricked into wrong position
- Collusion attacks using multiple, distributed provers

Hidden and Mobile Stations (Verifiers): hide position of verifiers so prover does not know how it has to spoof

5. Broadcast Authentication

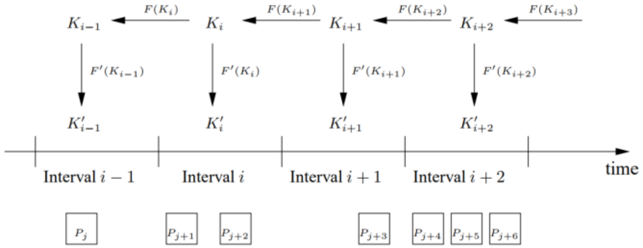
One sender, a number of receivers (possibly malicious)
- all receivers need to verify authenticity of message
- acknowledgement is not scalable

Public Key Encryption would work, but expensive
- device limited in memory and processing power
- signature verification is extremely expensive
- Asymmetric encryption takes seconds, whereas symmetric encryption only takes milliseconds

Main characteristics:
- purely symmetric primitives (MACs)
- asymmetry from delayed key disclosure
- One-way hash chains ("self-authenticating keys")
- requires loose time synchronization

5.1 TESLA – Delayed Key Disclosure

One-way hash chain: if know s_i, can easily generate s_{i-1}



- Sender generates a key K_l and keeps it confidential
- Generate K_0 and distribute it to all receivers

To transmit a message M_i, the sender MAC's M_i with the key of the current time interval K_i' which is only used within its interval & only disclosed after it

Always verify that the key is only used during its interval (as publicly disclosed afterwards, it is invalid later on)
- use different K / K' for **key generation & usage**

5.2 Integrity Codes (Presence awareness)

The receiver in direct power range of sender, and *knows it*!
- receiver knows a communication channel
- sender is always on and transmitting

Transmission: spread m to $2 * k$ bits: $1 \rightarrow 10, 0 \rightarrow 01$
- transmit using on-off keying (1 is random signal)
- complementary coding (e.g. Manchester)

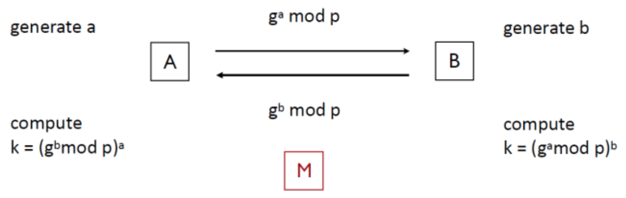
Reception: presence of signal interpreted as 1, else 0
- if half of the received bits are 1, not modified during transmission (can only add signal, not destroy it)
- can detect all modifications of the message

Use i-delimiters to signal start and end of message
- allows for arbitrary message sizes
- Manchester coding optimal "111000"

Integrity code is slow, can use e.g. as a separate channel for transmitting hash of message (integrity check)

5.3 Device Pairing

Diffie-Hellman Protocol



Vulnerable to Man-in-the-Middle (MitM) attacks

- use short-string comparison
- use public-key crypto (known public key, compare)
- use proximity ("if near me, comes from a friend")
- use physical contact (or pressed button, accelerometer)

6. Physical Layer Security

6.1 Channel-Based Key Establishment

Multipath: channel exhibits time-varying, stochastic & reciprocal fading; channels $> \lambda/2$ apart are uncorrelated

Reciprocity: channel looks exactly the same in both directions, "shared secret" out of thin air
- *Confidentiality*, as only received at intended location
- requires $\lambda/2$ accuracy on antenna, else channel changed

1. *Signal Acquisition & Quantization* (need exact same bits)
2. *Reconciliation* (error correction)
3. *Key confirmation* (check we have the same key)

No authentication, just confidentiality
- secret key establishment, but other party unknown
- need other method to authenticate
- attacker can influence and discover established key

Channel is modelled as single complex number (phase + amplitude) from point A to point B
- each pair of antenna has individual channel
- can be found with passive attacks & known plaintext

Zero forcing

Assumed that sender knows all channels (know attacker)

Given channel matrix *H*, find transmission filter *F* s.t.
- all valid receivers will get confidential data
- all unwanted receivers will have no (useful) data

Orthogonal Blinding

Sender does not know location of attackers
- use beamforming (spatial diversity) to guide data

Create jamming noise (included in data matrix *D*) so that at all positions except for intended one, will receive data + jamming signal as attacker and cannot read data

6.2 Friendly Jamming

Friendly jamming: transmit noise which the receiver subtracts so that only the intended receiver can subtract it by knowing the seed used to generate the noise

Jammer must be near to data source ($< \lambda/2$), as else channels are uncorrelated and attacker can separate
- data and jamming signal seem to come from same source

Possible for attacker with *multiple antenna to cancel noise*:
- two antenna use phase difference of $\lambda/2$ between jammer signals to eliminate jamming and only get valid signal (as same distance to original source)

However, still works well for **access control**: simply overload your own receiver as long as you don't want someone to access it ("wireless firewall")

6.3 Signal manipulation

Attacker can influence the channel itself

Artificial multipath: create artificial additional signal which suppresses the transmitted signal at the receiver

→ Can only use physical-layer schemes as *complementary measures for confidentiality*, as easily tricked
- however, well suited for access control schemes

7. Cellular Networks

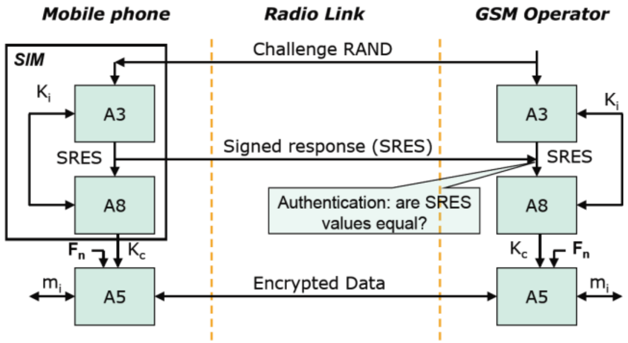
Primary security goals:
- Access Control
- Confidentiality

7.1 GSM (2G)

Most widely used cellular standard, $> 600m$ users
- 900 MHz band, 25MHz subdivided into 124 channels
- cell size up to 35km, BS differ in used frequencies

Based on TDMA radio access in-between users
- 8 speech channels per frequency channel (200 kHz)
-uses SS7 signalling with mobile-specific extensions

Operators build strong client authentication to protect itself from billing fraud, but **no network authentication**
- *Subscriber Identification Module* (SIM)
- Subscriber Authentication Key (K_i) of 128 bits
- *International Mobile Subscriber Identity* (IMSI)
- PIN allows SIM card to activate itself



A5: Encryption (standardized)
- provides confidentiality (integrity implicit in human)

A8: Key generation (can be operator-specific)
- provides authentication & session key

SRES: "Message authentication codes"

Home Location Register (HLR): provides *Mobile Switching Center* (MSC) with required data (RAND, SRES, K_c)

Visitor Location Register (VLR): stores triple when not at home; no access to subscriber key K_i

K_i is stored on the SIM card itself and contains all knowledge about the user; can be used to clone SIM

Problems:
- one-way authentication (network simply trusted)
- encryption only for part of the message & weak
- no integrity check (okay for voice, bad for data)

7.2 Signaling System 7 (SS7)

Protocol suit used by most telecommunication service providers to talk to each other

Service providers trust each other → **no authentication!**

Attacks

Location Tracking: use *paging* to find serving cell tower

Denial of Service: using knowledge of IMSI and VLR, can control service availability & disable functionality at will

Call interception: relay call over your own base station

7.3 UMTS (3G)

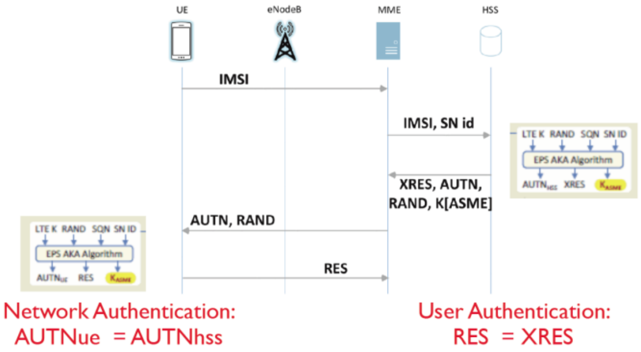
Reuse of 2nd generation security principles (GSM)
- removable hardware security module (SIM)

But: **limited trust in Visited Network**
- **Two-way authentication** of both user *and* station
- IMSI only **temporary**, not fixed anymore (no tracking)
- Protection of end-user identity (don't tell ID)
- Generate MACs and Keys only based on user key, which can then be sent over the network
- key generation based on *Rijndael* (and published!), but operators can choose their own ones if wanted

Correction of previous weaknesses:
- no more attacks from fake base stations
- always use encryption for entire message
- provide data integrity (not only voice anymore)

But: ISMI sent *in cleartext* first time user is in new network
- MitM & Hijacking still possible with disabled encryption

7.4 LTE (4G)



Two-way authentication: user **and** network authentication
- 3 choices of algorithms which are all publicly known

Renegotiation attack: possible to use weaknesses of previous by downgrading to GSM with weak A5/1

Localization attack: passive attacker can sniff paging requests over the air and then force UE to attach to rogue BS and get fine location through reconfiguration requests

7.5 Authentication in Telephony Networks

Protocols change as the call is established and propagates throughout the network, flow is modified (e.g. codec)

AuthLoop: use standard TLS handshake
- original TLS takes a long time (100s) to complete
- use stripped down version
- need to use FSK as else too much interference along transmission path in network

8. Key Distribution

Interesting Property for Sensor Networks
- multi-hop network to relay messages
- no infrastructure which can be relied upon

Primary security goal:
- Authentication

Symmetric & Public Key

Public-Key infrastructure would be simple, but expensive

1. Public-Key (PK) for everything
+ simple key distribution, simple broadcast authentication
- sensors need to do PK, expensive memory & processing

2. PK for key establishment, then SK for rest
+ simple key distribution, fast with SK
- no efficient broadcast, need to be able to do PK and SK

3. Symmetric Key (SK) for everything
+ need to perform only SK, very fast & efficient crypto
- key distribution difficult, no efficient broadcast

Key distribution

1 key for all: efficient broadcast, vulnerable to compromise

1 key for each pair: expensive, no broadcast mechanism

Subsets of keys: rather cheap, resilience to compromise
- each node just gets a subset of all keys, high probability that it has one for each other node to communicate over

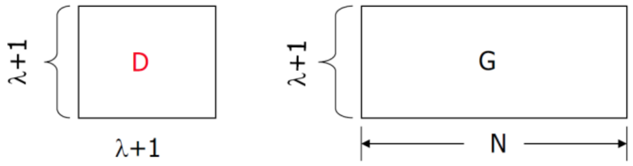
Key graph G_k : connected if share at least one key
- better connected → increased security, as shared key

Key sharing graph G_{sk} : connected if within range & share
- better connected → increased vulnerability as can listen

Larger key pool size → better resilience
Smaller key pool size → better connectivity

Deterministic approaches

N nodes, λ rank of matrix (tolerate up to λ compromises)



G: *public* matrix
D: *private* matrix (symmetric), only known to system

$$A = (D\ G)^T$$

All columns of A must be linearly independent in order to prevent collusion in-between nodes to impersonate others

Each node N_i knows the ith row of matrix K:

$$K = A\ G = (A\ G)^T \rightarrow K_{ij} = K_{ji}$$

To communicate with another node K_j, it simply takes the corresponding value K_{ij} which is known to both parties

9. Secure Routing

Dynamic Source Routing (DSR)

On-demand source routing protocol
- **route discovery:** request route and read replies
- **route maintenance:** detect route errors

Position-based greedy forwarding

Route to destination based on known position:
- *Most Forward within Radius* (MFR)
- *Nearest with Forward Progress* (NFP)
- Compass forwarding

Attacks

Worm holing: attract all traffic and simply dump it

State corruption: create invalid message to confuse nodes

Modification / Creation: create and change packets

Congestion: create congestion / overload on other nodes so that they consume more / unnecessary resources

Mitigation

Secure Routing Protocol (SRP)
Use symmetric-key authentication (MACs) with shared keys between source and destination
- all links authenticated using shared keys
- still, mutable fields can be changed at will (e.g. hops)

Ariadne
- add own name to the hash to show path taken
- sign entire packet to verify origin
- can also use standard MACs on each link or TESLA

10. Various

$$1\ dBm = \ dB\ /\ 1\ milliwatt\ (mW)$$

$$1\ dBW = \ dB\ /\ 1 \qquad Watt\ (W)$$

dBi: dB value of antenna gain relative to gain of isotropic antenna ($0dBi \ \cong isotropic\ antenna$)

Logarithms

$$N(dB) = 10 * log_{10}(N)$$
$$N(dBm) = 10 * log_{10}\left(\frac{N}{1mW}\right)$$