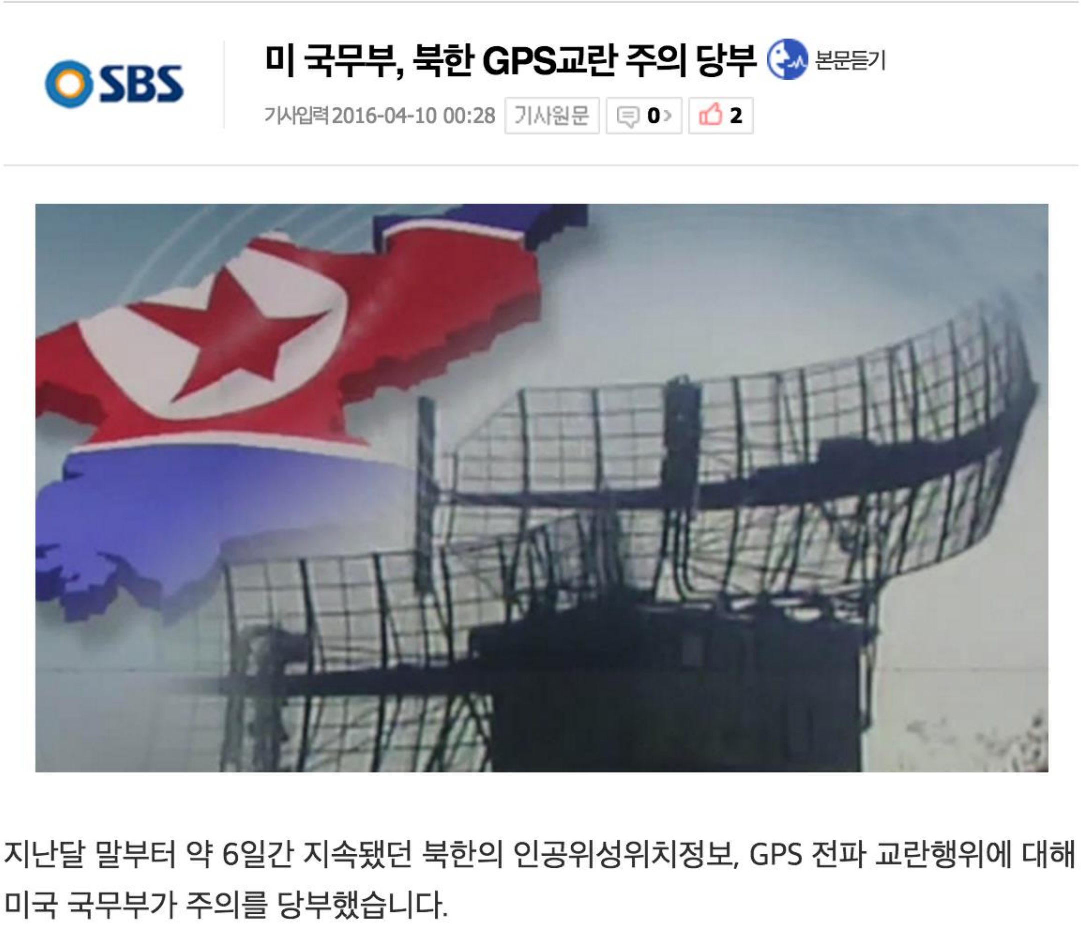
GPS Spoofing Attack

System Security Lab.

Juhwan Noh

GPS

북한 GPS 전파 교란



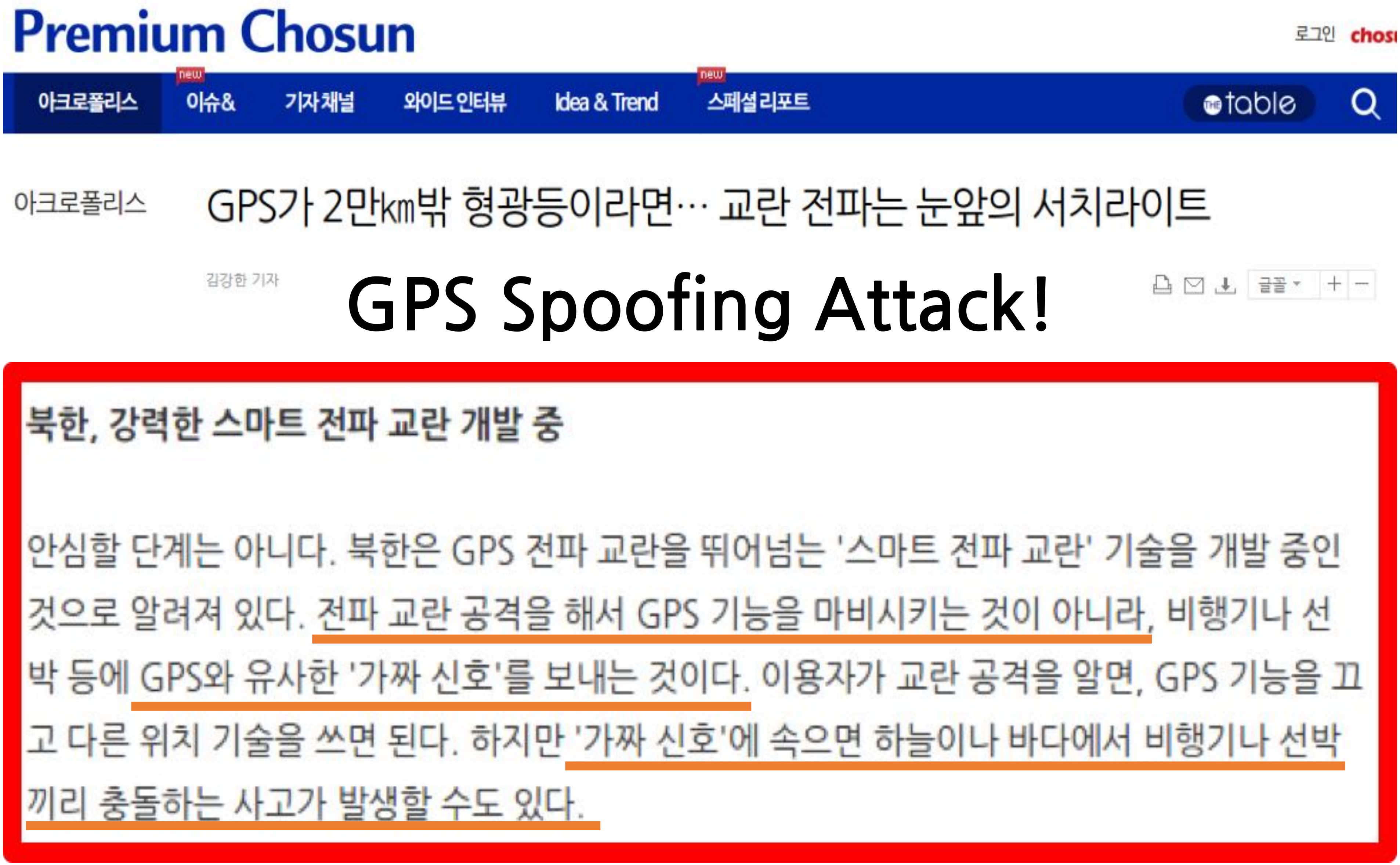
SBS

미 국무부, 북한 GPS교란 주의 당부 본문듣기

기사입력 2016-04-10 00:28 기사원문 0 2

지난달 말부터 약 6일간 지속됐던 북한의 인공위성위치정보, GPS 전파 교란행위에 대해 미국 국무부가 주의를 당부했습니다.

GPS Spoofing Attack!



아크로폴리스

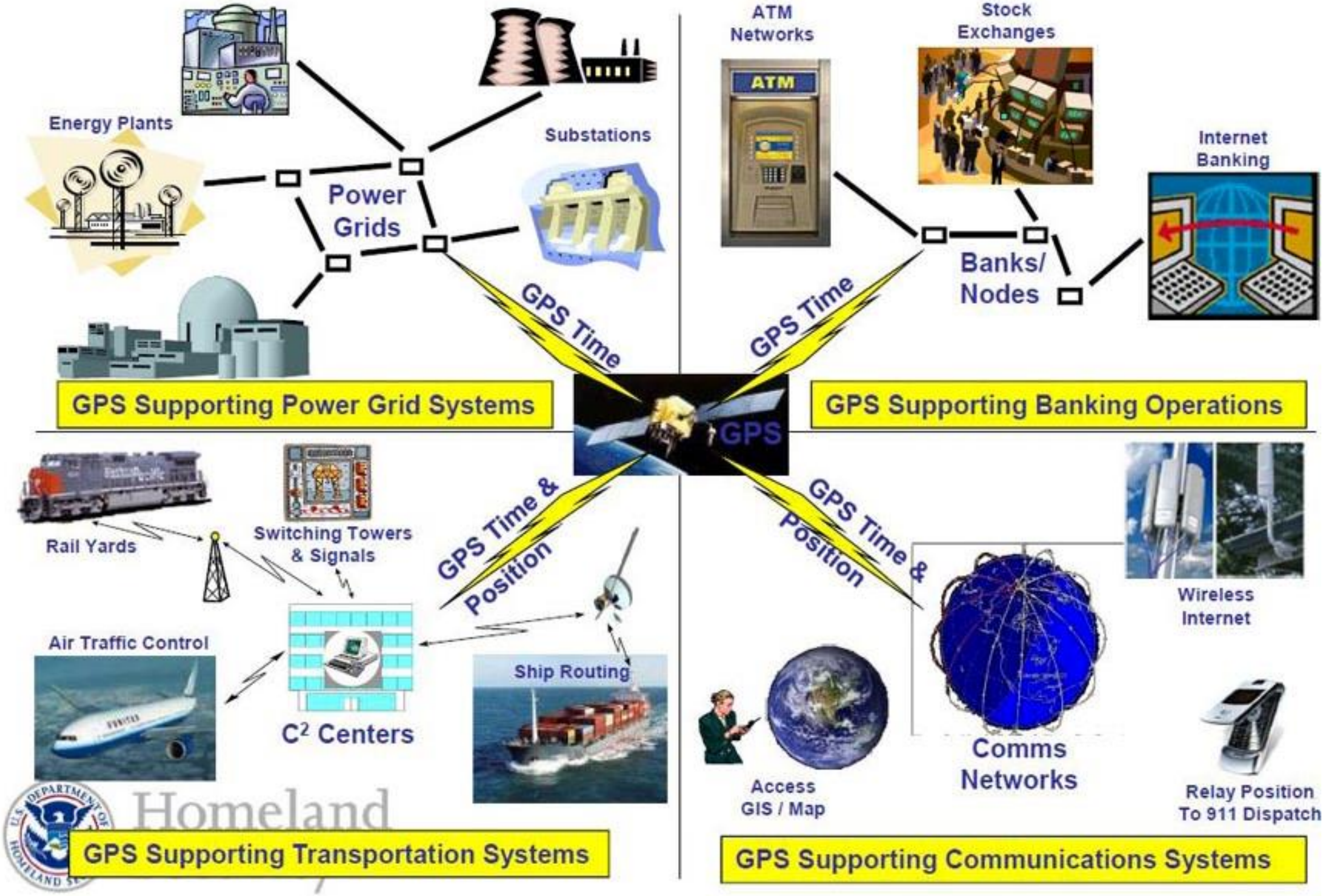
GPS가 2만㎞밖 형광등이라면… 교란 전파는 눈앞의 서치라이트

김강한 기자

북한, 강력한 스마트 전파 교란 개발 중

안심할 단계는 아니다. 북한은 GPS 전파 교란을 뛰어넘는 '스마트 전파 교란' 기술을 개발 중인 것으로 알려져 있다. 전파 교란 공격을 해서 GPS 기능을 마비시키는 것이 아니라, 비행기나 선박 등에 GPS와 유사한 '가짜 신호'를 보내는 것이다. 이용자가 교란 공격을 알면, GPS 기능을 끄고 다른 위치 기술을 쓰면 된다. 하지만 '가짜 신호'에 속으면 하늘이나 바다에서 비행기나 선박끼리 충돌하는 사고가 발생할 수도 있다.

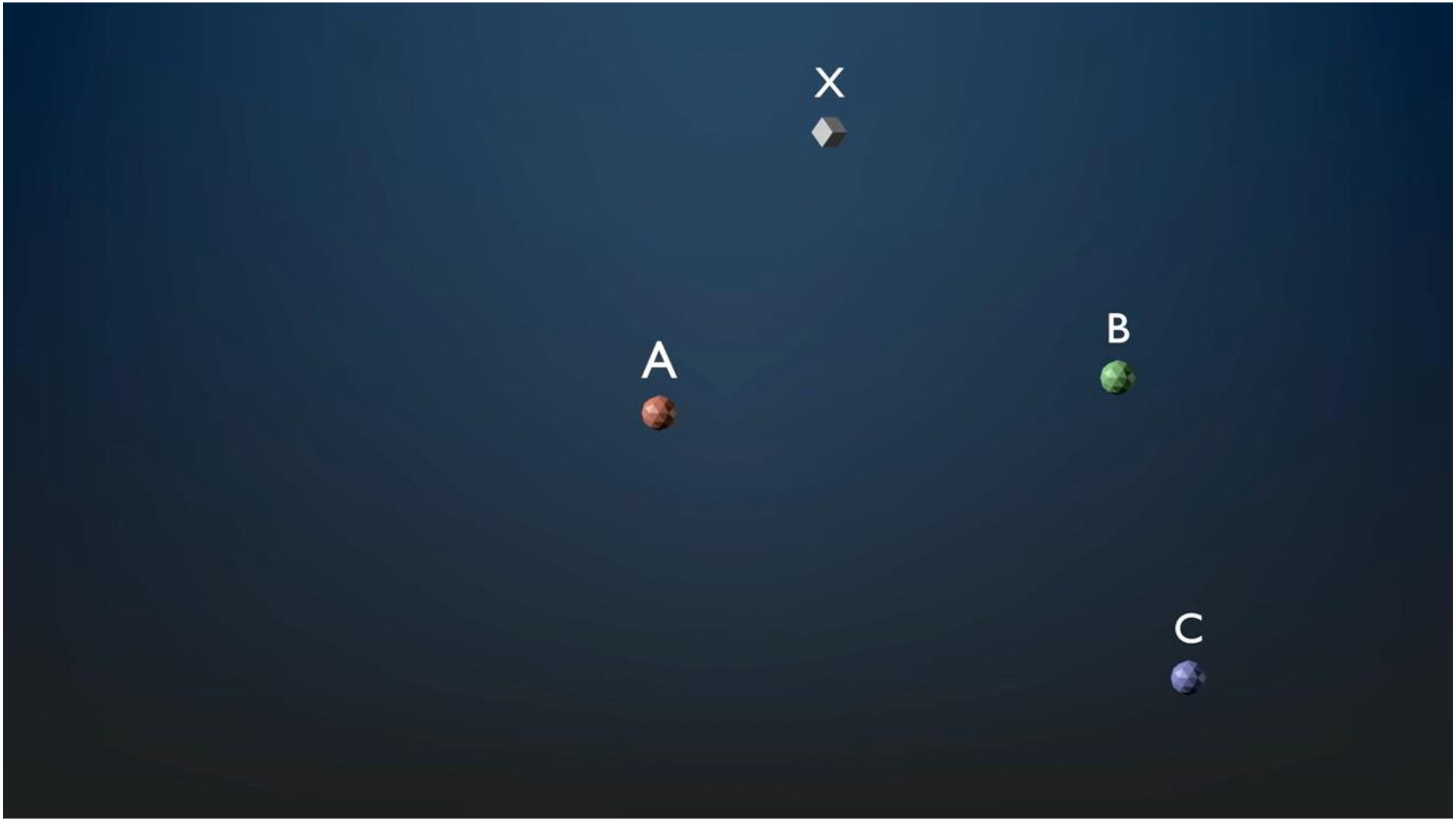
Extent of GPS Dependencies



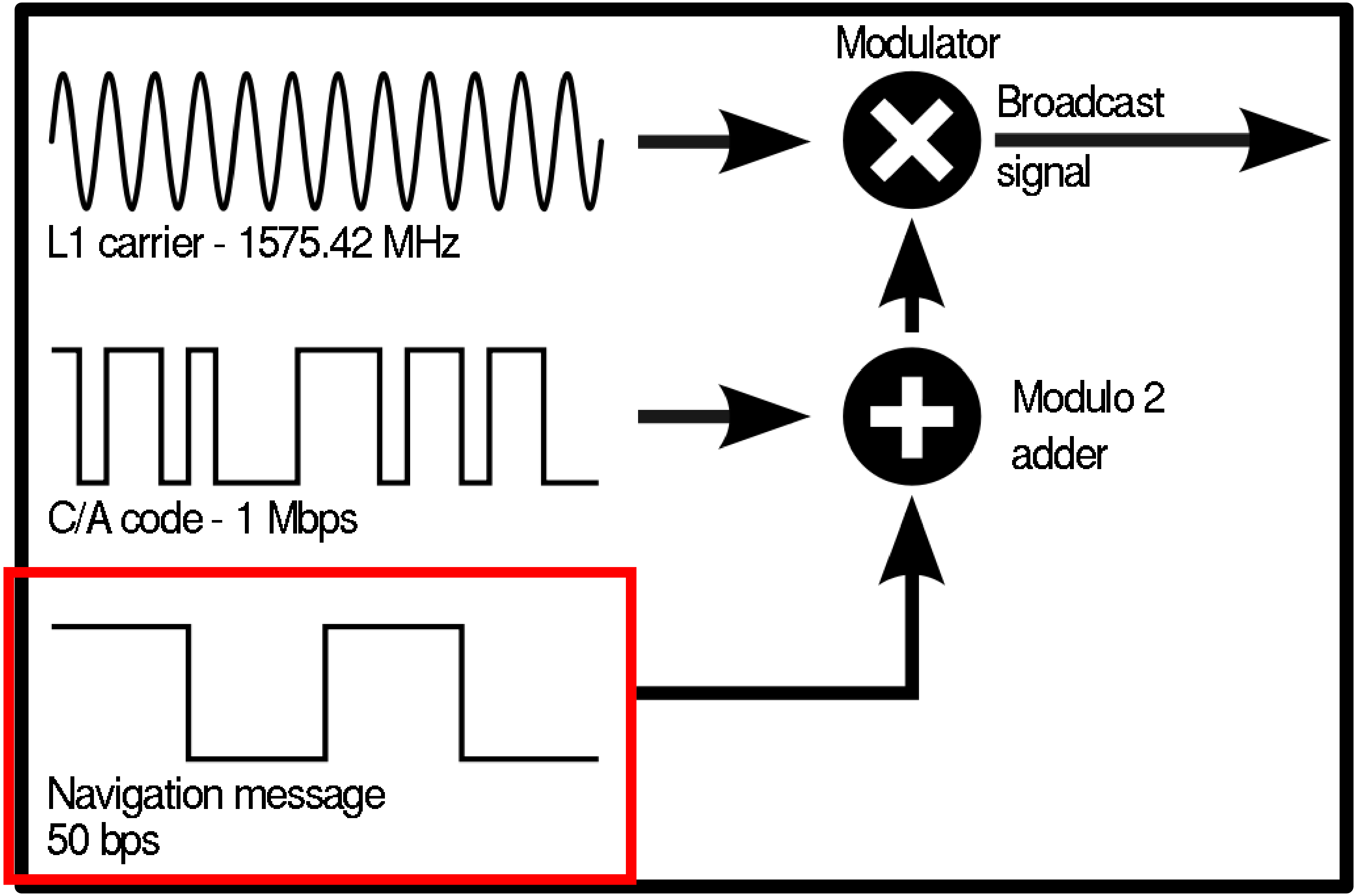
National Risk Estimate: Risks to U.S. Critical Infrastructure from GPS Disruption, The U.S. Department of Homeland Security, 2013

GPS Spoofing Attack

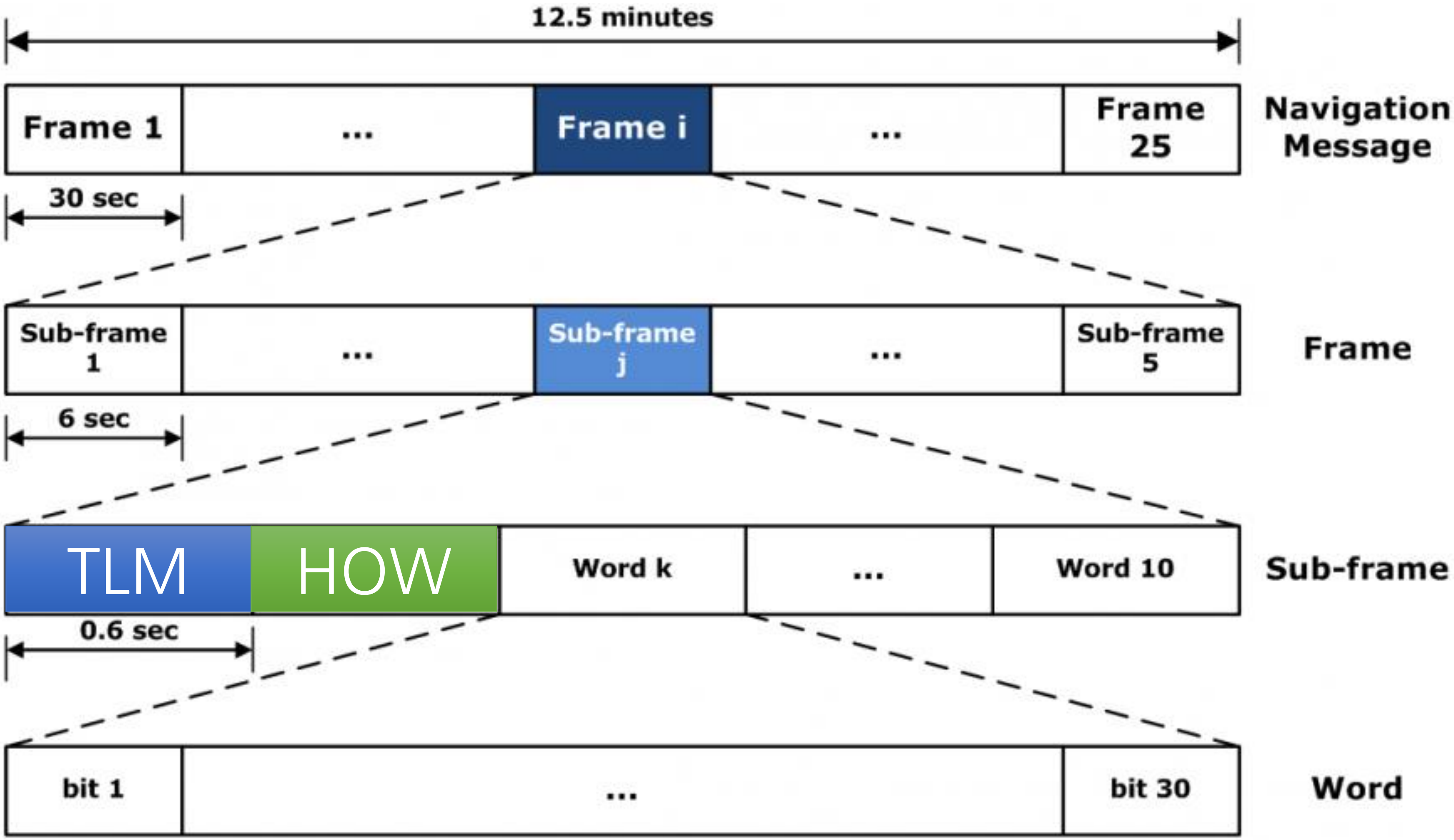
GPS



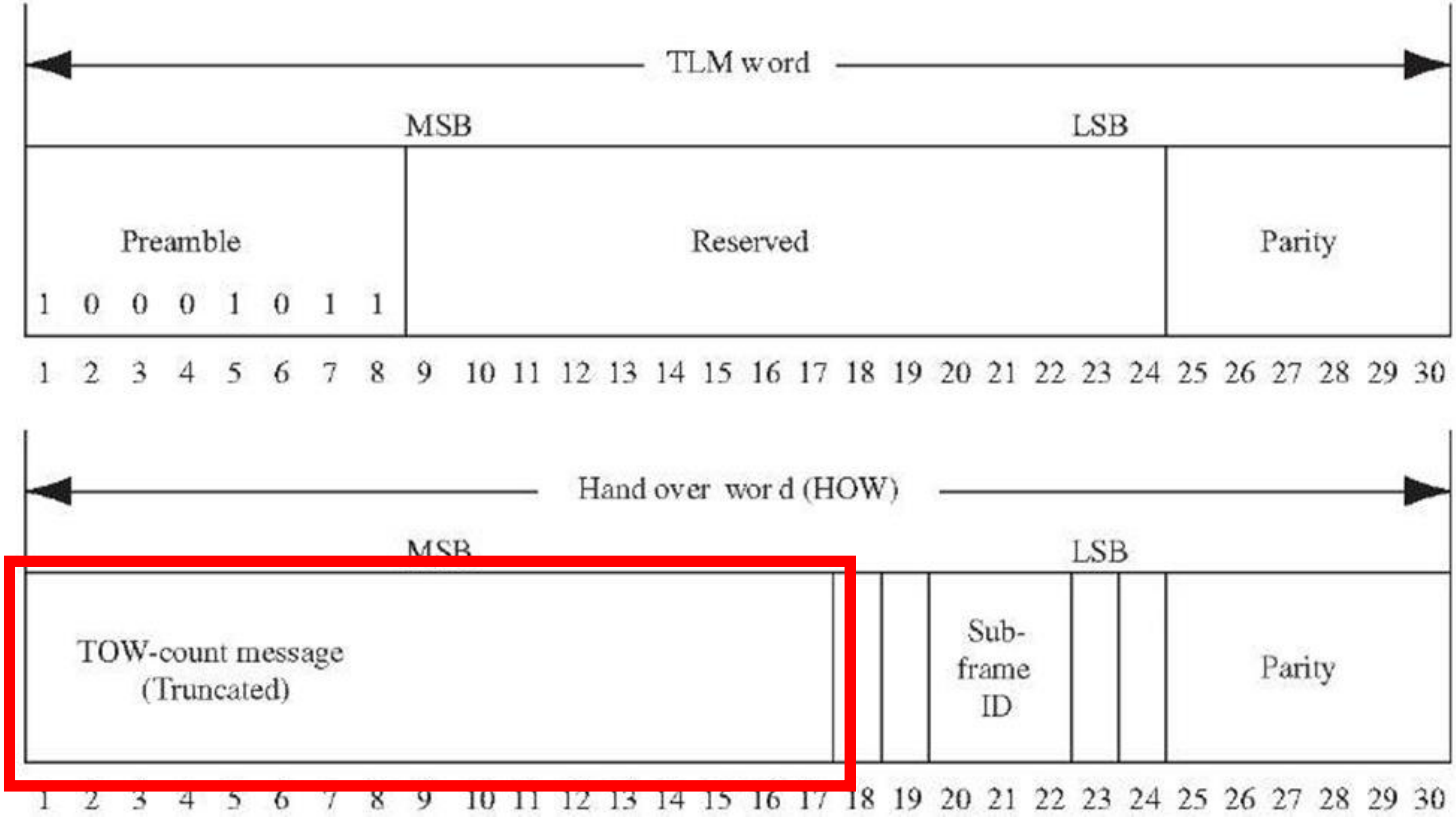
GPS Broadcast Signal



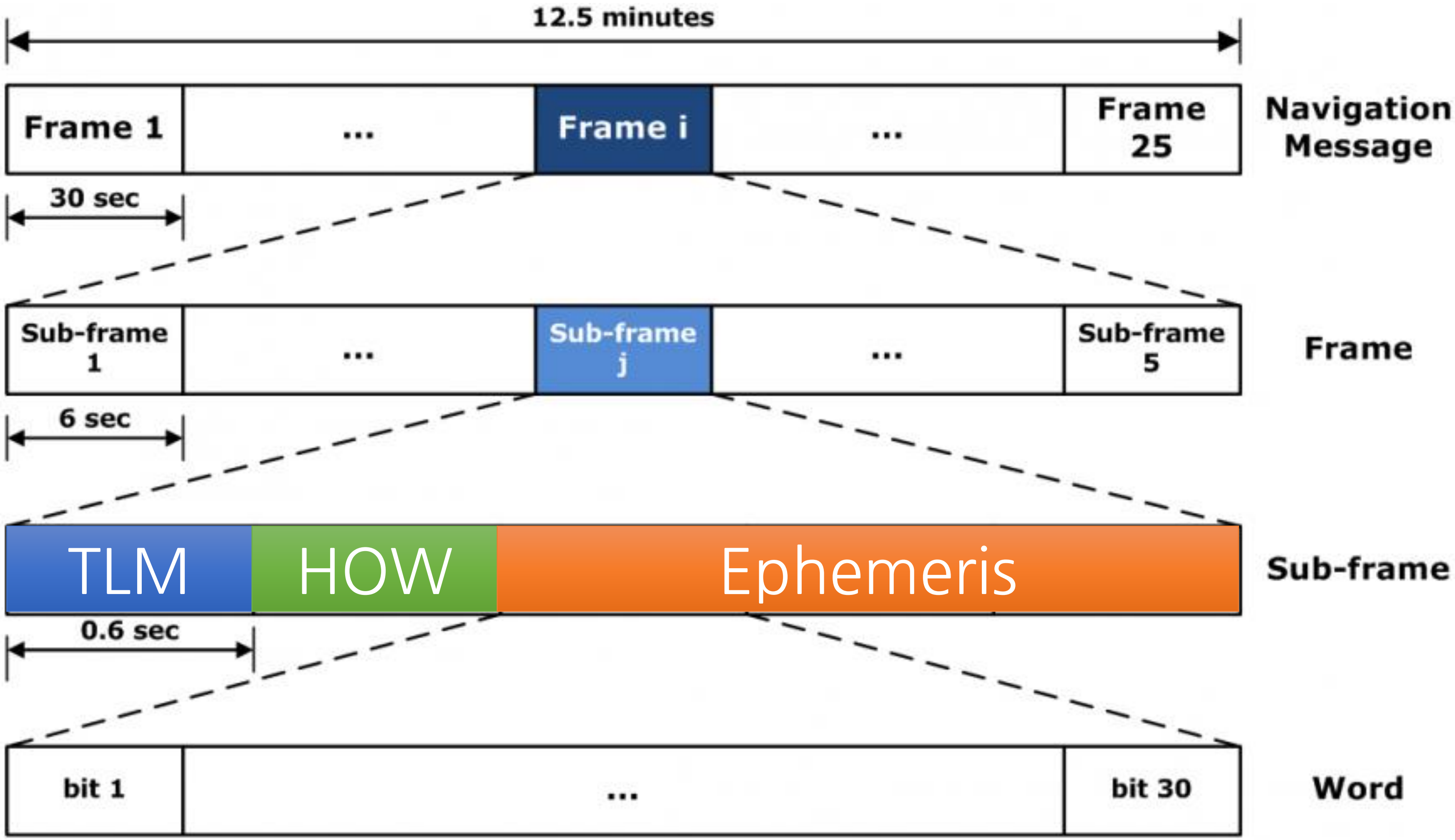
Navigation Message



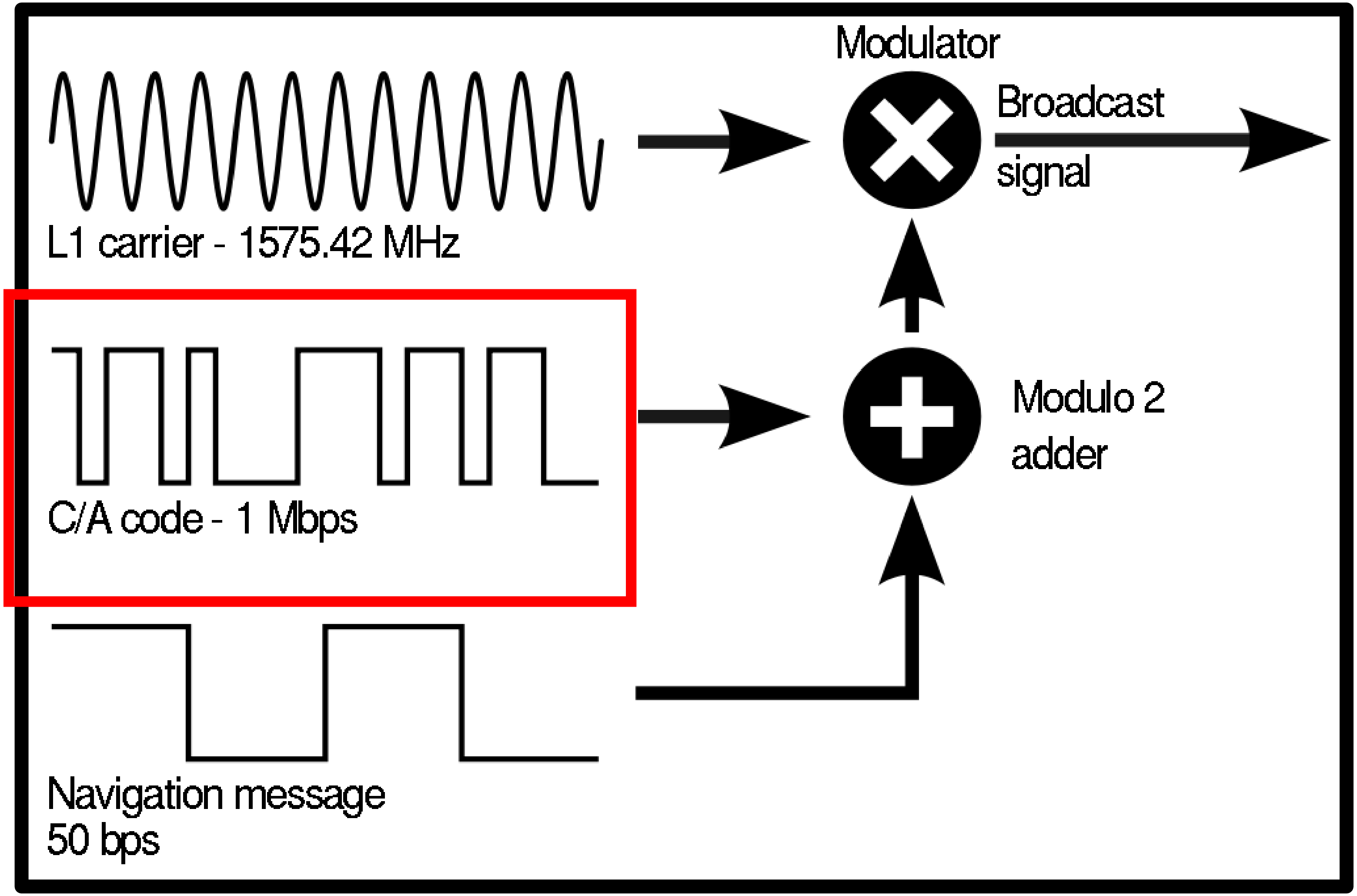
TLM & HOW


TLM word
MSB
LSB
Preamble
1 0 0 0 1 0 1 1
Reserved
Parity
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Hand over wor d (HOW)
MSB
LSB
TOW-count message
(Truncated)
Sub-
frame
ID
Parity
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

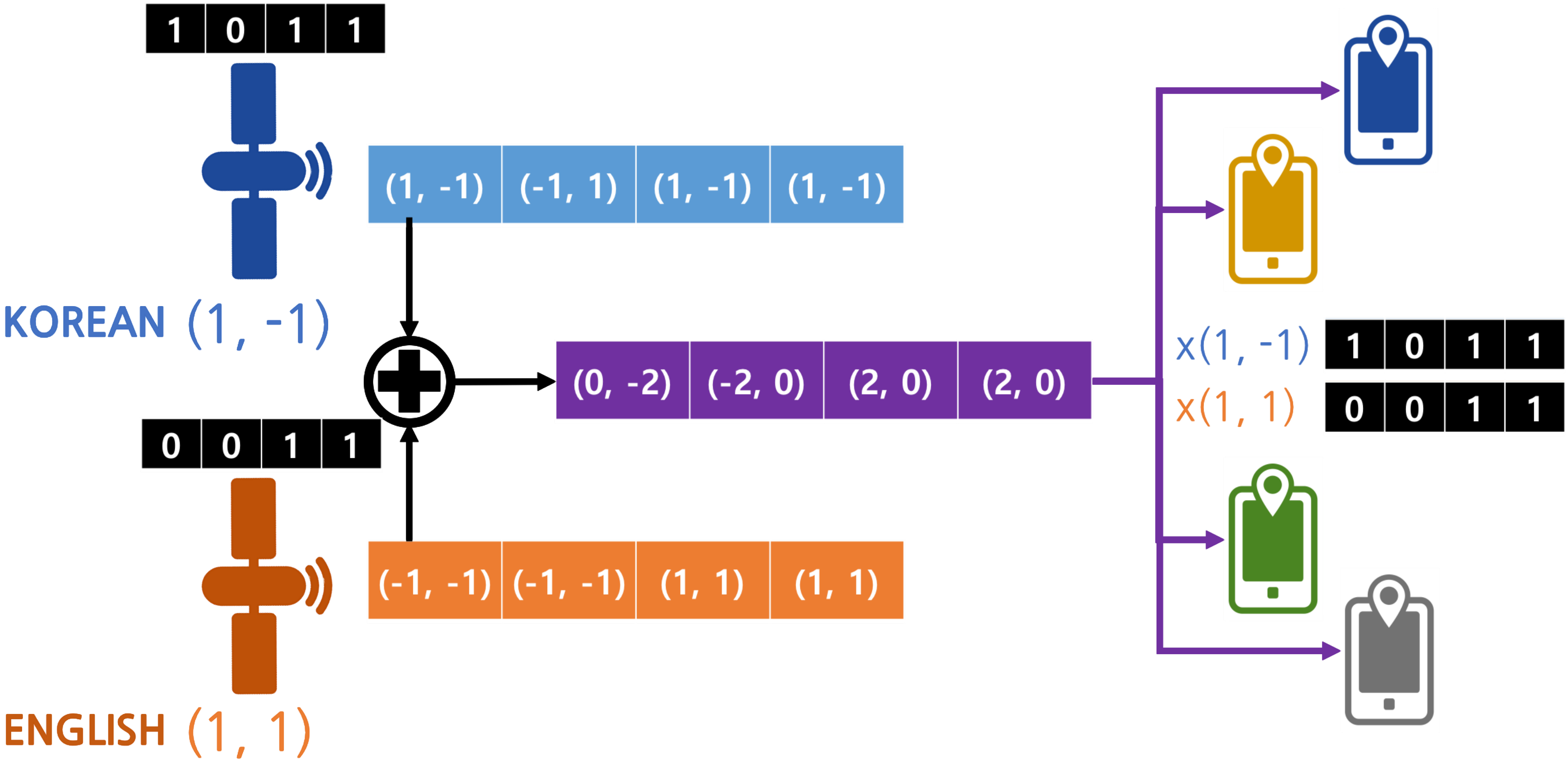
Navigation Message



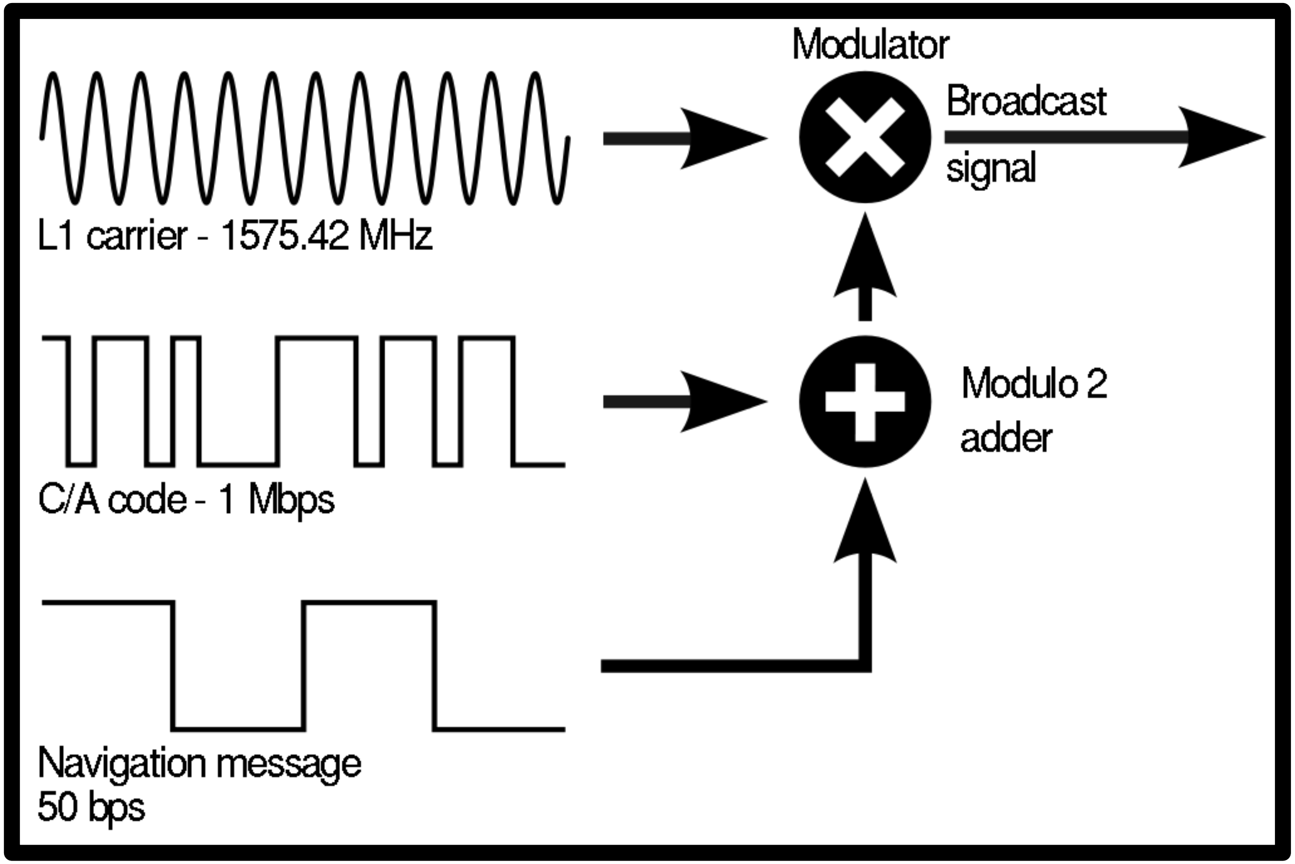
GPS Broadcast Signal



C/A code


1 0 1 1
(1, -1)
(-1, 1)
(1, -1)
(1, -1)
KOREAN (1, -1)
(0, -2)
(-2, 0)
(2, 0)
(2, 0)
x(1, -1)
1 0 1 1
x(1, 1)
0 0 1 1
0 0 1 1
(-1, -1)
(-1, -1)
(1, 1)
(1, 1)
ENGLISH (1, 1)

Civilian GPS Is Vulnerable



No authentication & No encryption

On the Requirements for Successful GPS Spoofing Attack

Nils Ole Tippenhauer, Christina Pöpper, Kasper B. Rasmussen, Srdjan Capkun

18th ACM Conference on Computer and Communications Security (CCS 2011)

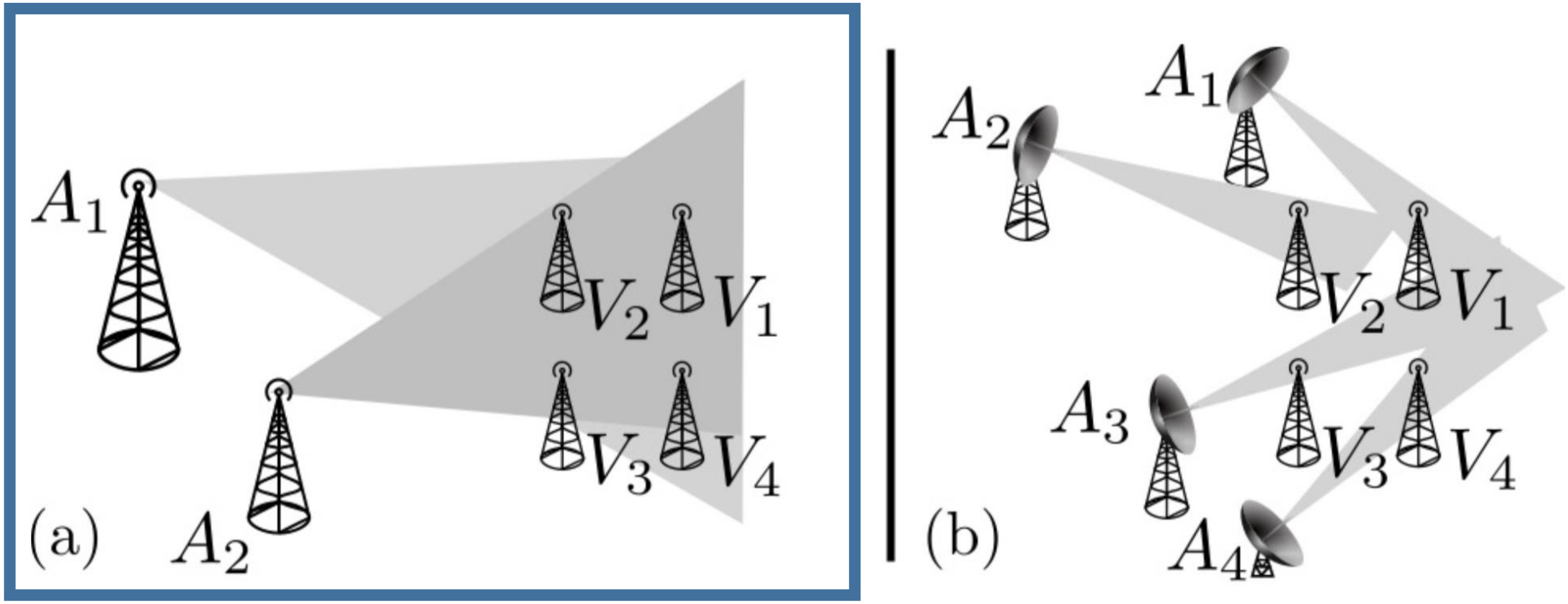
Presented by Juhwan Noh

Motivation

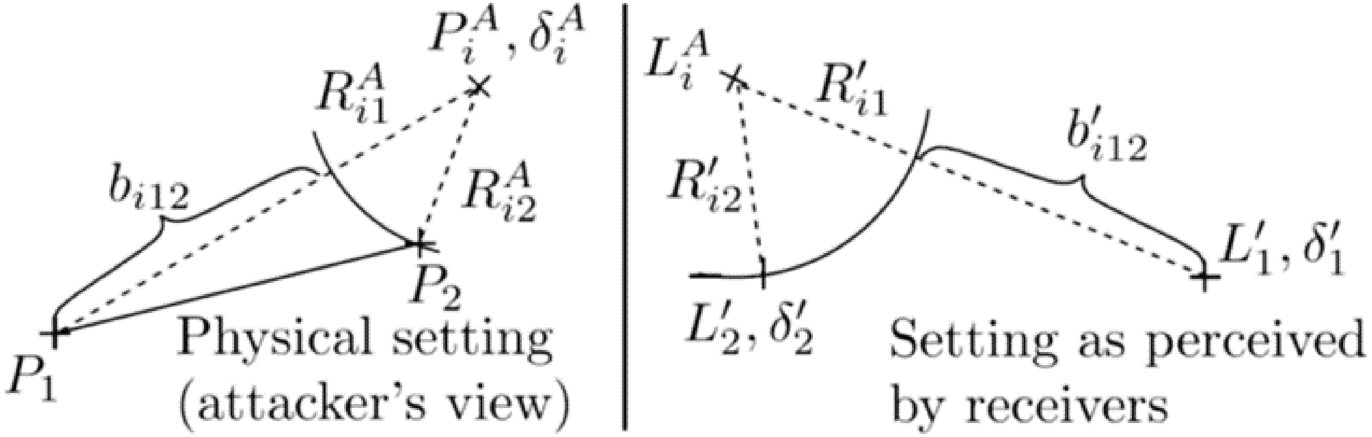
- Analysis on the necessary conditions for the successful GPS spoofing attacks
  - Physical location of an adversary
  - Inaccuracies in these parameters

Basic research on effective receiver-based countermeasures

Attacker Model



Solution

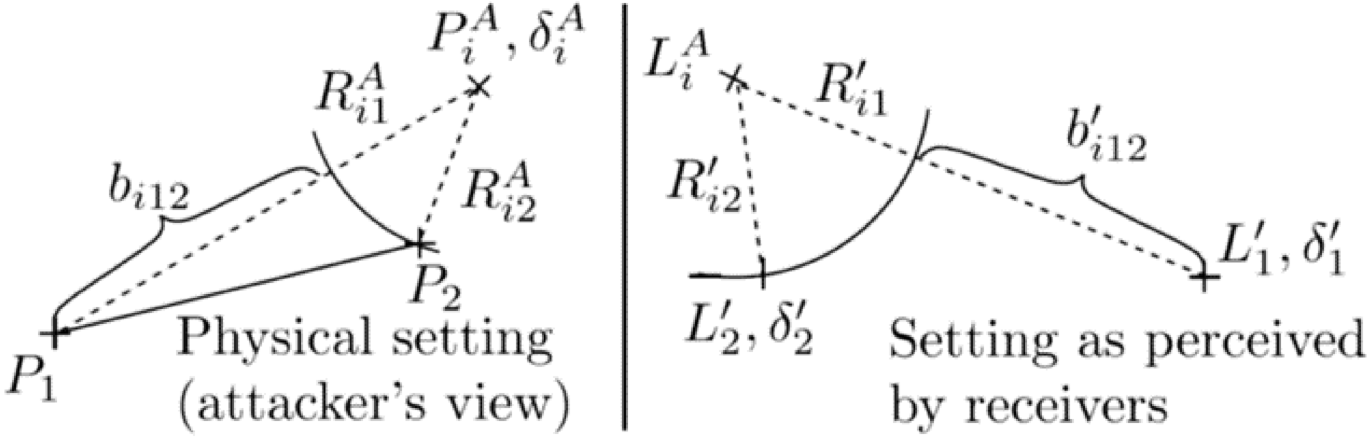


❖Pseudorange

- Physical: ${R_{ij}}^A = \left|P_j - {P_i}^A\right| + {\Delta_i}^A$
- Logical: $R'_{ij} = \left|L'_j - {L_i}^A\right| + \Delta'_j$

❖Free to choose attacker's physical location, forged location, and time offset

Solution



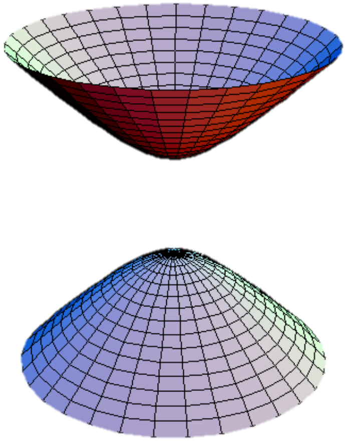
❖Difference btw two pseudoranges from each receivers

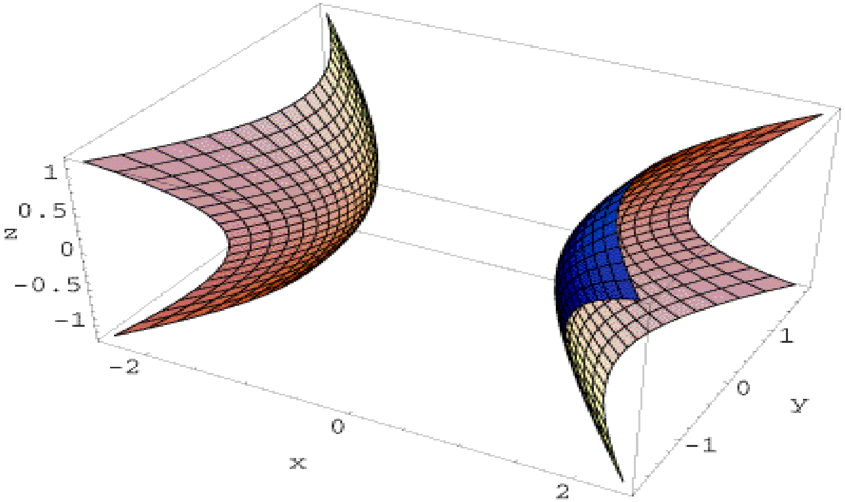
- $b_{ijk} = |P_j - {P_i}^A| - |P_k - {P_i}^A|$
- $b'_{ijk} = \left|L_j - {L_i}^A\right| - \left|L_k - {L_i}^A\right| + \Delta'_j - \Delta'_k$

❖$\underline{b_{ijk} = b'_{ijk}}$ in order to preserve formation

Result

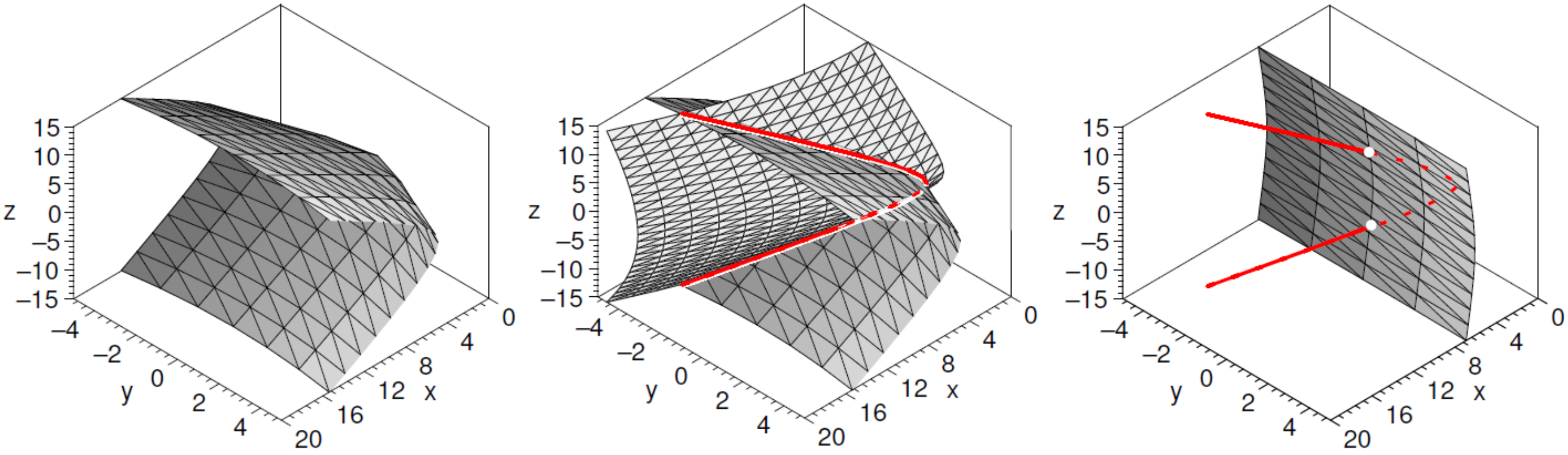
- ❖Multiple receivers can be spoofed to the same location with different time offset
  - If receivers share relative distances among them or its time offset → can detect attacks
- ❖Two receivers can be spoofed to the different location
  - To avoid detection, attacker should lie on one half of a two-sheeted hyperboloid(AP-BP = constant)





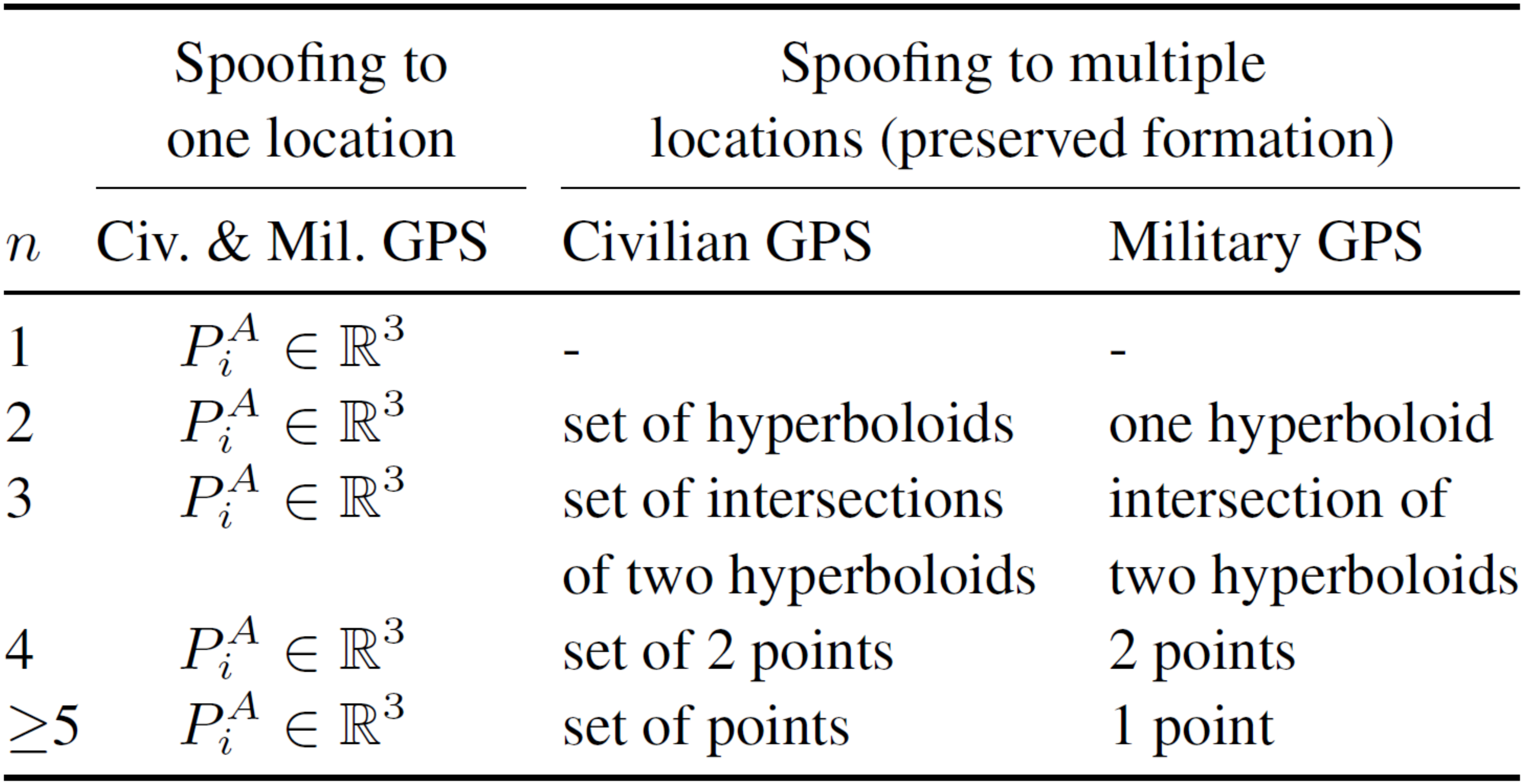
Result

- ❖Three receivers can be spoofed to the different location
  - To avoid detection, attacker should lie on the intersection of two hyperboloids defined by b'_{i12}, b'_{i13}
- ❖More than three receivers can be spoofed to the different location
  - To avoid detection, attacker should lie on the intersection points of (n-1) hyperboloids defined by b'_{i12}, b'_{i13}, …, b'_{i1n}



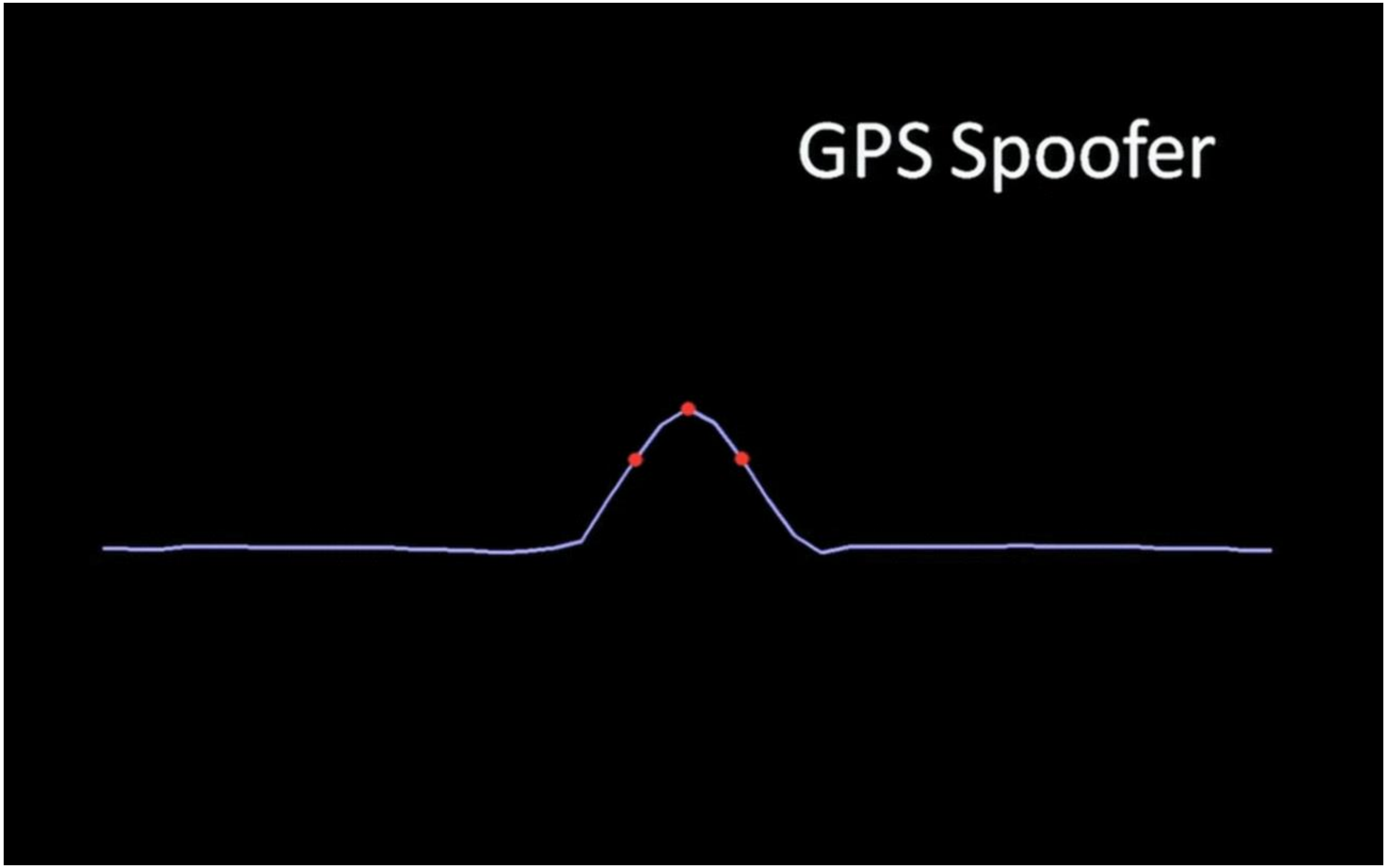
(a) 2 receivers (b) 3 receivers (c) 4 receivers

Result

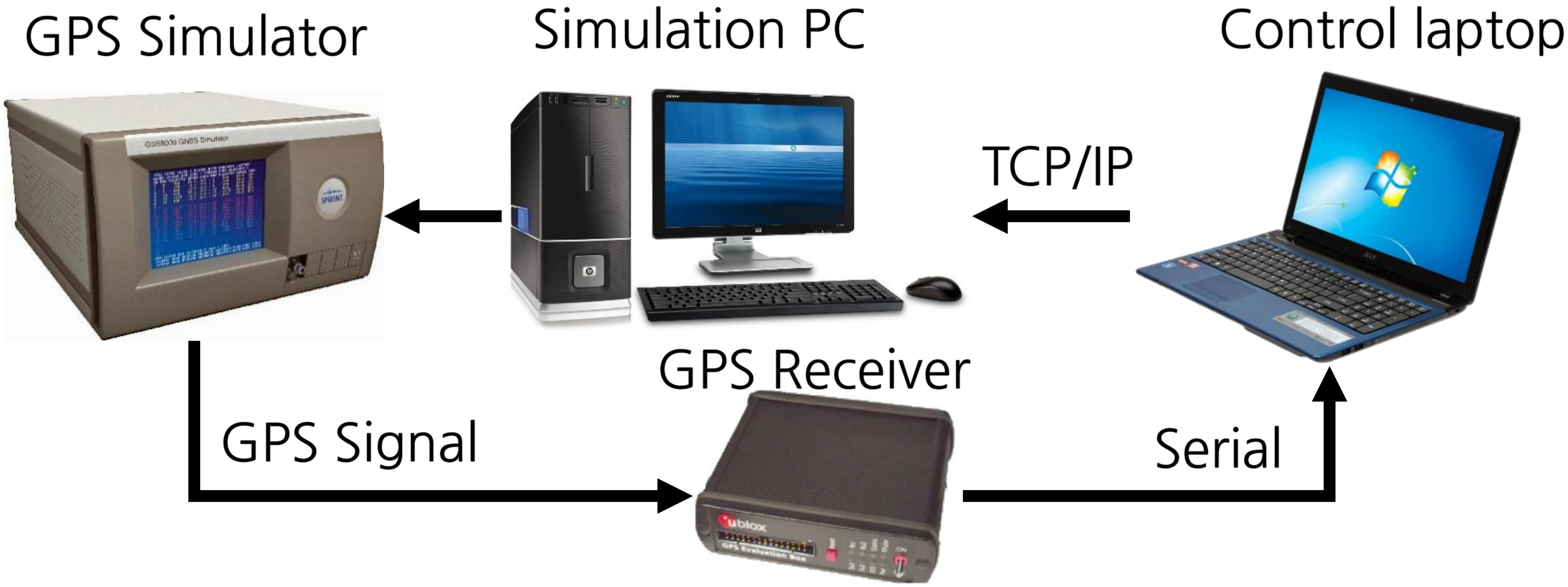


	Spoofing to one location	Spoofing to multiple locations (preserved formation)	
n	Civ. & Mil. GPS	Civilian GPS	Military GPS
1	$P_i^A \in \mathbb{R}^3$	-	-
2	$P_i^A \in \mathbb{R}^3$	set of hyperboloids	one hyperboloid
3	$P_i^A \in \mathbb{R}^3$	set of intersections of two hyperboloids	intersection of two hyperboloids
4	$P_i^A \in \mathbb{R}^3$	set of 2 points	2 points
$\geq$5	$P_i^A \in \mathbb{R}^3$	set of points	1 point

How to invade a GPS receiver without getting caught



Experimental Setup



GPS Simulator

Simulation PC

Control laptop

TCP/IP

GPS Receiver

GPS Signal

Serial

- The acceleration: $0.5m/s^2$
- Consider the takeover succeeded
  - Height difference < 150m, horizontal distance < 1km

Summary of results

	Parameter value required for successful spoofing
Relative signal power	≥ +2dB
Constant time offset	≤ 75ns
Location offset	≤ 100m
Relative time offset	≤ 80ns

Countermeasure

- ❖Exchange GPS receivers' individual GPS locations with one another
  - Possible space for placements of attacker's antenna gets reduced as the number of receivers increase

Conclusion

❖Attacker should satisfy the requirements:

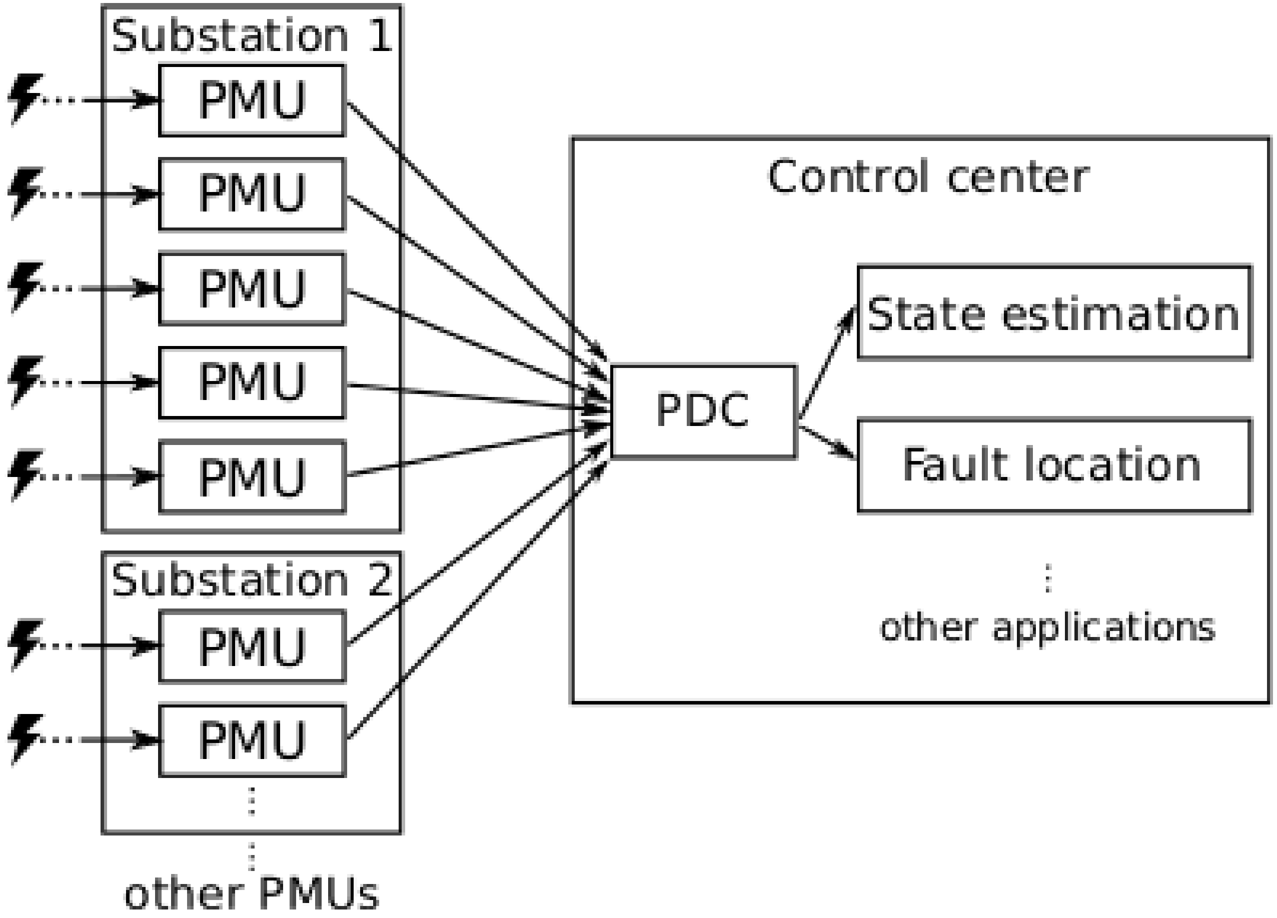
- Relative position of attacker's antennas depends on location & formation of GPS receivers
- Relative signal power, constant time offset, location offset and relative time offset

Short Paper: Detection of GPS Spoofing Attacks in Power Grids

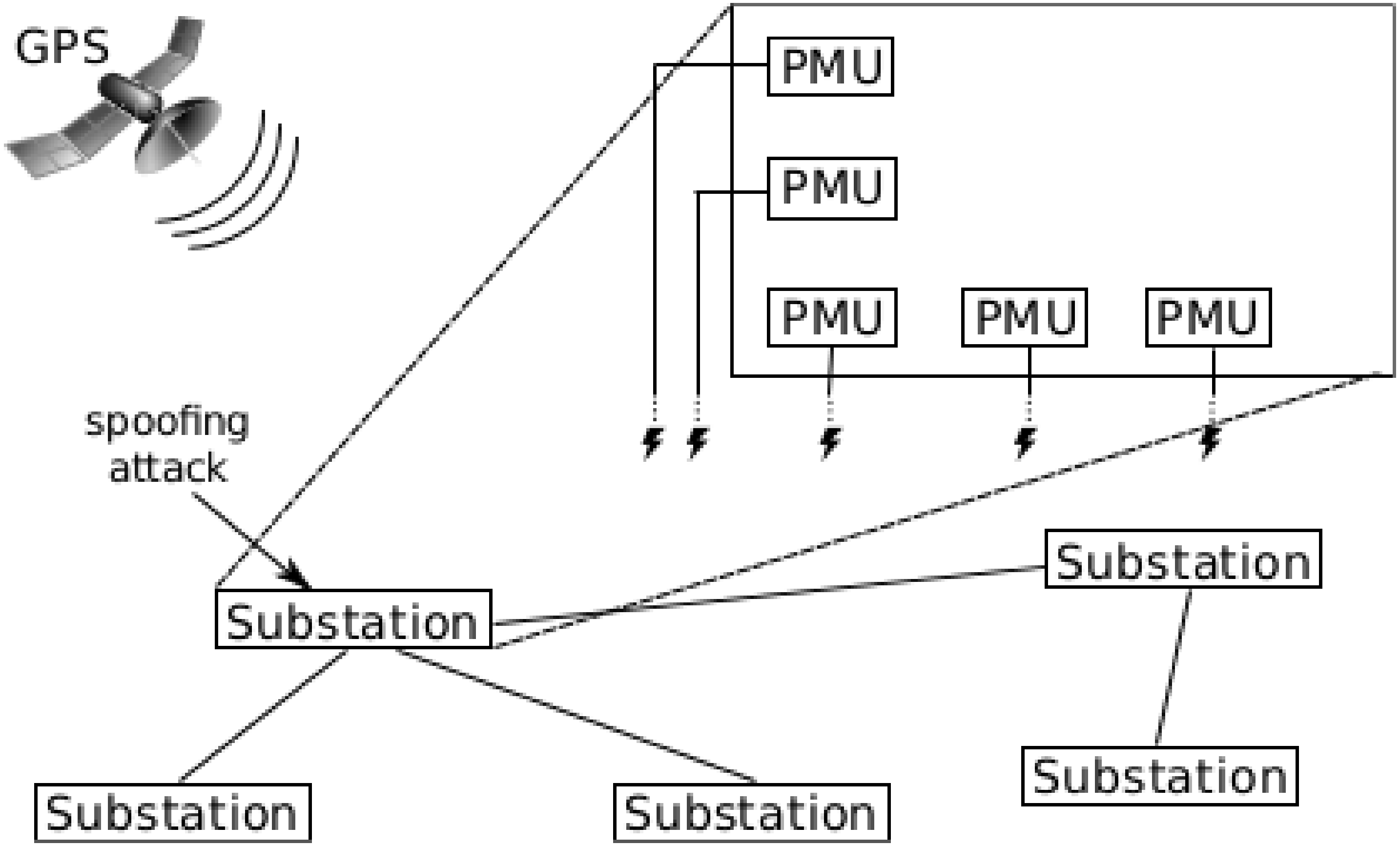
Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher,
Srdjan Capkun, David Basin

The 7th ACM Conference on Security and Privacy in Wireless and
Mobile Networks (WiSec 2014)

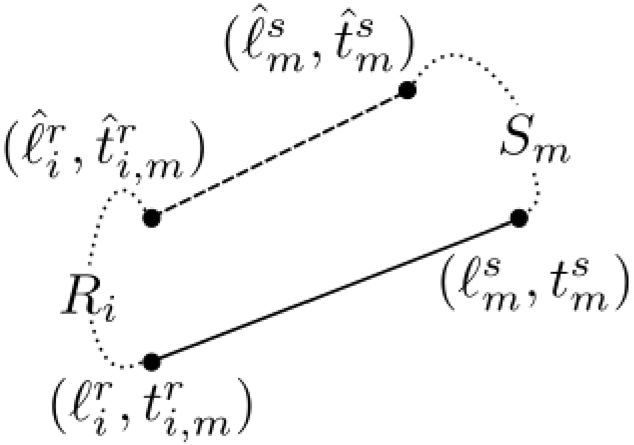
Power Grids


Substation 1
PMU
PMU
PMU
PMU
PMU
Substation 2
PMU
PMU
other PMUs
Control center
PDC
State estimation
Fault location
other applications

Power Grids


GPS
PMU
PMU
PMU
PMU
PMU
spoofing attack
Substation
Substation
Substation
Substation
Substation

Requirements for Attack Detection


$(\hat{\ell}^s_m, \hat{t}^s_m)$
$(\hat{\ell}^r_i, \hat{t}^r_{i,m})$
S_m
R_i
(ℓ^s_m, t^s_m)
$(\ell^r_i, t^r_{i,m})$

❖Message content verification: $(\widehat{l^s_m}, \widehat{t^s_m})$ are fixed

❖Receiver location verification: $\widehat{l^r_i} = l^r_i$

❖Grouped receivers clock offset verification

- 1 free variable, $\delta^r_{i,m}$

❖Single receiver clock offset verification

- n_r-n_{rc} free variables, $\delta^r_{i,m}$

Q&A