A Security Framework for Mobile Business to Mobile Customer Services

Shu Chen, Yingying Chen †, Wade Trappe**

**WINLAB, Rutgers, The State University of New Jersey*

†Dept. of ECE, Stevens Institute of Technology

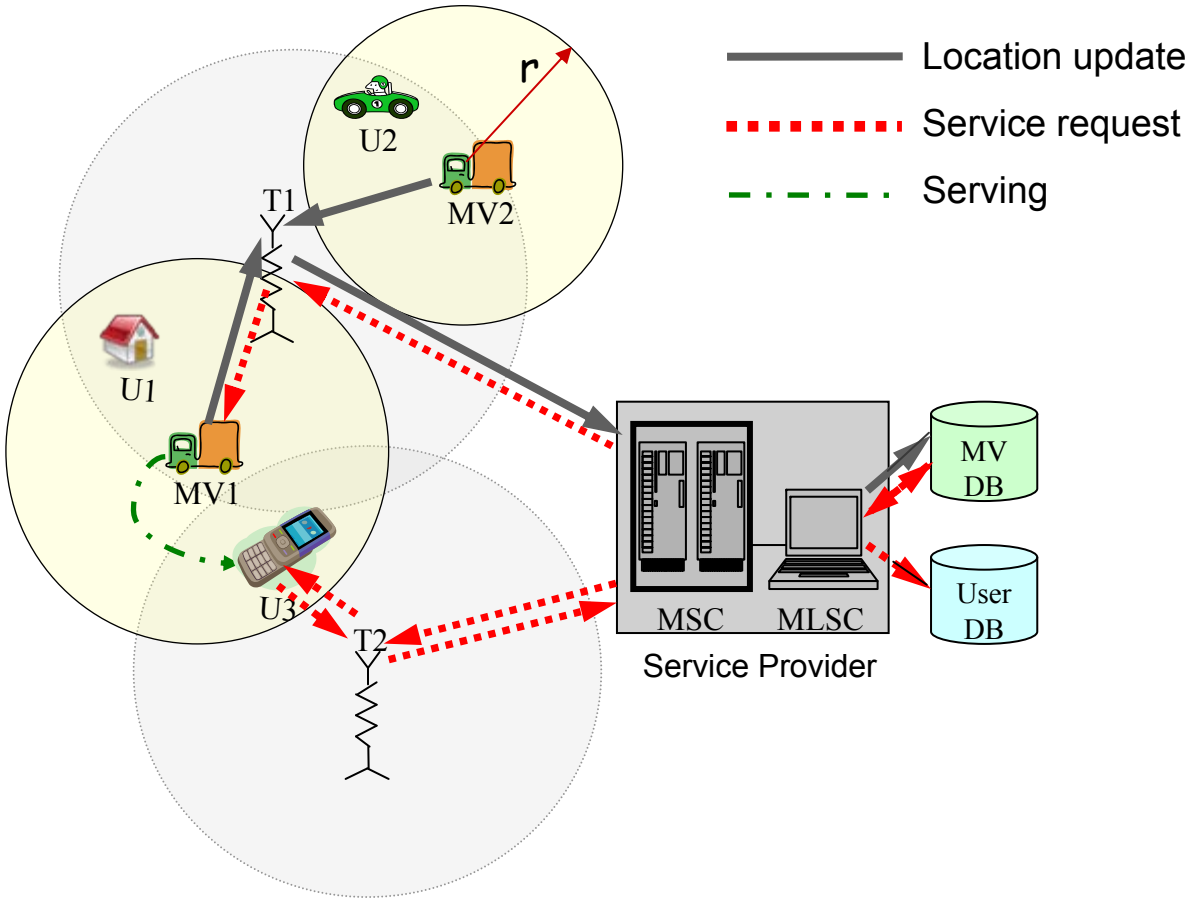
Outline

- Introduction
  - Basic Mobile Location-based Services (MLS) Architecture
- Security Threats
- Main Techniques
  - Location Verification
  - Cryptographic Protocols
- A Security Framework for MLS

Mobile Location-based Services (MLS)

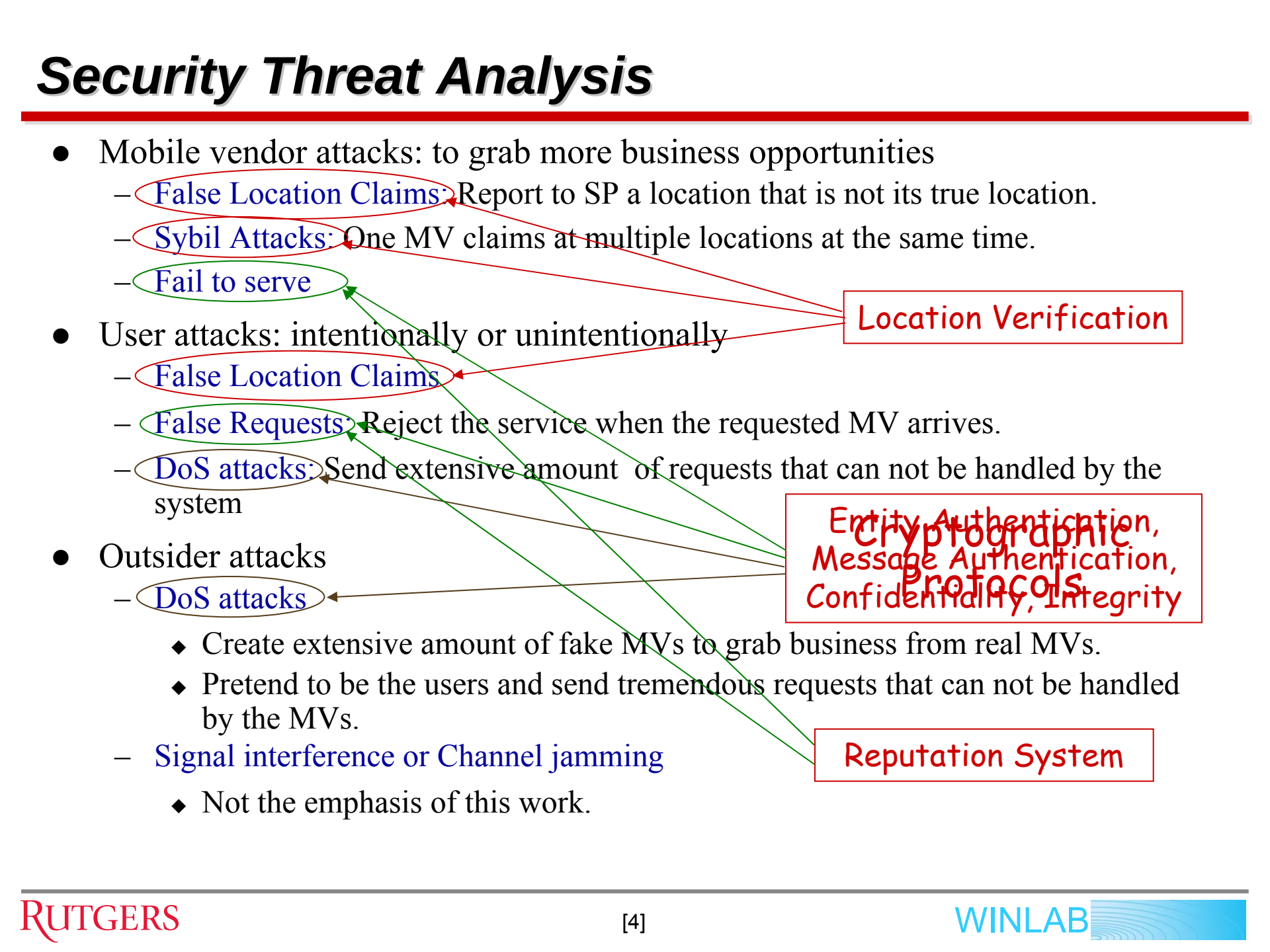
- Services provided by cellular network operators that facilitate the communications between the mobile business vendors and the potential mobile customers.

- Mobile Vendors (MV):
  - Service radius *r*
  - Constantly update locations to the Service Providers
- Users (U)
  - GPS-enabled devices
  - Report location to SP when request services.
- Service Providers (SP)
  - Network Operators
  - Service Center (MLSC), Databases



Security Threat Analysis

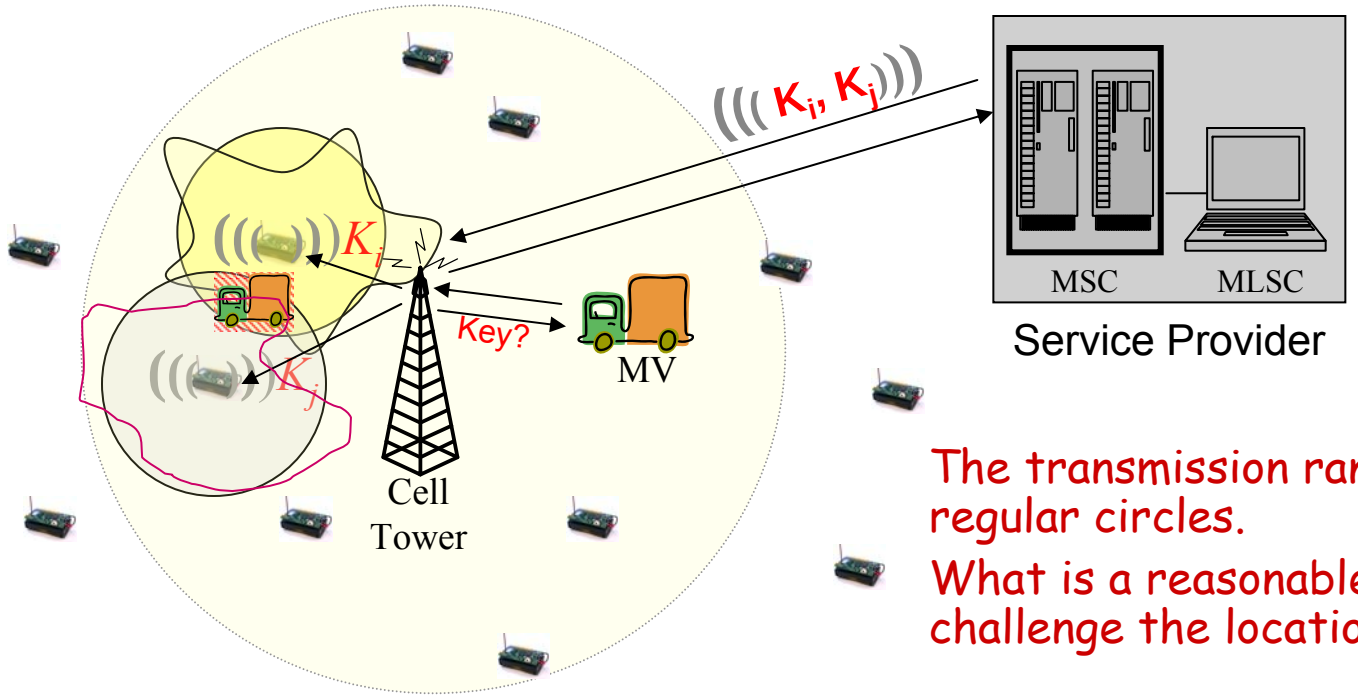
- Mobile vendor attacks: to grab more business opportunities
  - False Location Claims: Report to SP a location that is not its true location.
  - Sybil Attacks: One MV claims at multiple locations at the same time.
  - Fail to serve
- User attacks: intentionally or unintentionally
  - False Location Claims
  - False Requests: Reject the service when the requested MV arrives.
  - DoS attacks: Send extensive amount of requests that can not be handled by the system
- Outsider attacks
  - DoS attacks
    - Create extensive amount of fake MVs to grab business from real MVs.
    - Pretend to be the users and send tremendous requests that can not be handled by the MVs.
  - Signal interference or Channel jamming
    - Not the emphasis of this work.



Location Verification

- Verify whether a location claim Loc_{now} sent to the SP by a MV or User is correct.
- Too costly to verify every location update.
- Two levels check: Simple and complex.
- Step 1: Consistency Check
  - *Consistent with historic location claims?*
    - *Set a threshold speed* MaxSpeed.
    - *A location claim* Loc_{now} *is suspicious* if $\frac{\| Loc_{now} - Loc_{old} \|}{| t_{now} - t_{old} |} > MaxSpeed$
  - *Consistent with cell tower information?*
    - *The cell tower that a mobile subscriber is currently associated is recorded in MSC.*
    - *If* $\text{Loc}_{\text{now}} \notin$ Cell(T), then Loc_{now} is suspicious.
  - Fast, low cost, but loose. Find the suspicious location claims and put to step 2.
- Step 2: Location Verification
  - Challenges:
    - *Cellular networks, unbounded area. Can not use indoor or local-area methods.*
    - *The location claimer is not trustworthy, can't rely on its report.*

Key Distribution based Location Verification Method (KDLV)



The transmission ranges are not regular circles.

What is a reasonable way to challenge the location claimer?

- Use an auxiliary network with higher density of transmitters, who communicate with the cellular system.
  - Access points in emerging cellular data service technique, which uses WiFi for data services.
  - *Hybrid Cellular-Ad hoc data services*
  - *RFID*
- *A challenge-response method*
  - SP distributes keys to the transmitters whose transmission range covers the claimed location. See [Chen06SASN] for detailed key scheduling.
  - Involved transmitters broadcast the assigned keys in their covered areas.
  - The location claimer has to provide the keys to prove that it is at its claimed location.

Investigate KDLV -- Objective and Model

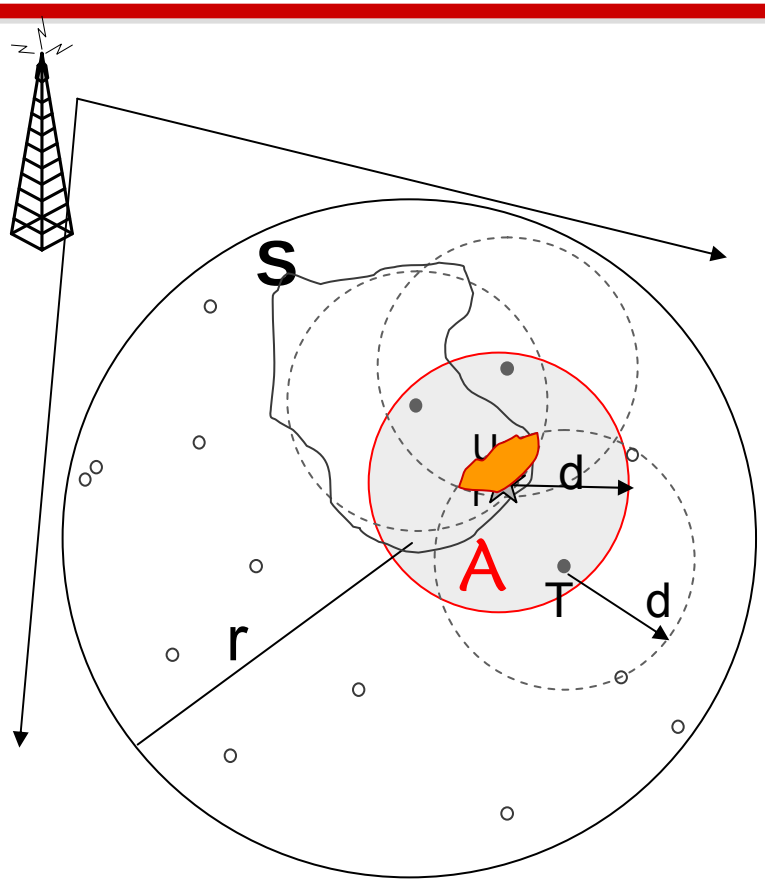
- **Objective:** Investigate the relationship between the required location accuracy and the deployment of the network. How dense should the transmitters be deployed given an acceptable error distance.

- **Deployment Model:** The transmitters deployed follow a Spatial Poisson Distribution in the whole area of interest S (e.g. a cell).
  - A: subset of S, |A| denotes the size of A.
  - λ: density of the transmitters
  - N(A) = # of transmitters in A.
  - Then, N(A) ~ Poisson(λ|A|) $P(N(A)=n)=\frac{e^{-\lambda}\lambda^{n}\,|A|^{n}}{n!}$

- **Propagation Model:** The log-distance path loss model.

$$PL(d)[dBm]=P_0-10\gamma\log_{10}\left(\frac{d}{d_0}\right)+X_\sigma$$

Investigate KDLV -- Approaches



Two steps:

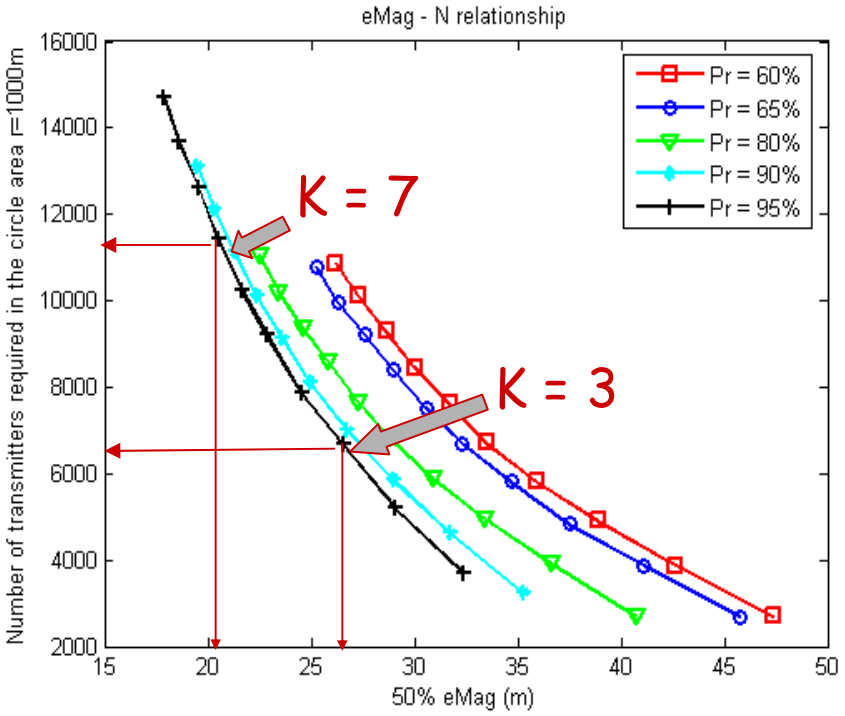
1. k-N relationship: In order to ensure a user to receive *k* keys at any location, with confidence α, how many total number of transmitters are required to be deployed?
2. k-eMag relationship: If the user received k keys, how accurate we can locate the user, in terms of error distance?

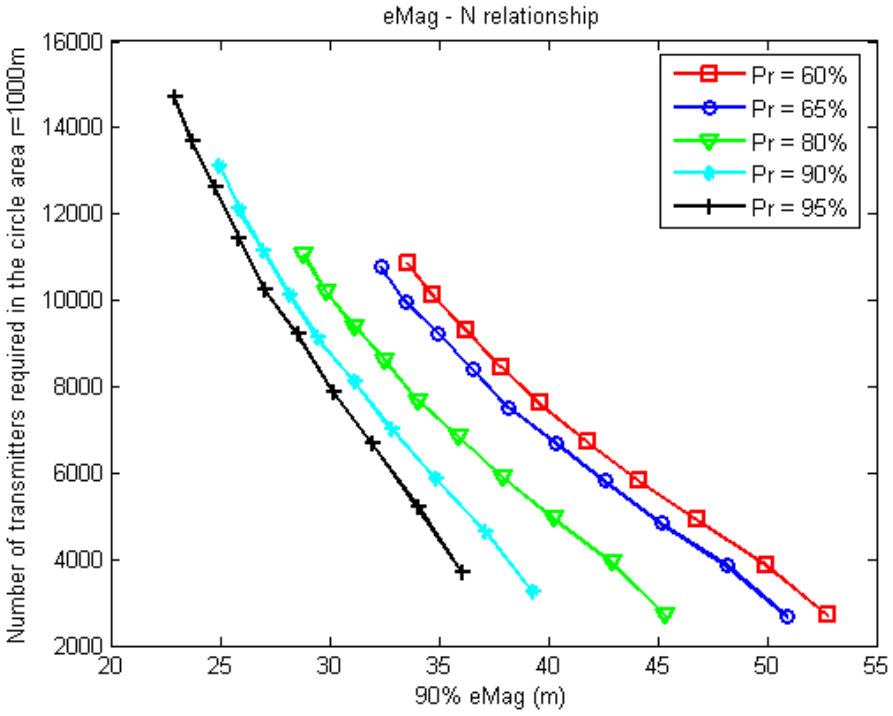
⇒ eMag-N relationship: eMag is the error distance I can bear, how many transmitters I need to deploy in S?

N: number of transmitters in S. $N = \lambda r^2$
k: the number of keys a user is required to receive.
eArea: size of area the user can be located within
eMag: = sqrt(eArea), magnitude of the error area.

eMag – N relationship

Combining k-N and k-eMeg together, we get eMag – N relationship, which shows if the requirement is to verify an entity within eMag distance (in *Pe percentage* of the cases), N transmitters are needed to be deployed in the whole region, with confidence α.





Transmission Power = 20dBM, α= 95%,

Cryptographic Protocols

1. Entity Authentication: An entity X (X can be MV, U or SP) is identified by a digital certificate $Cert_X^{CA}$, *PKI key pair* (KU_X,KR_X), obtained from a Certificate Authority.

$$Cert_X^{CA} = E_{KR_{CA}}[ID_X, KU_X]$$

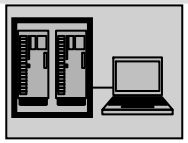
2. MV/user exchanges a session key, and key for Message Authentication Code (MAC) with the SP, using *Cert* and *PKI key pairs*.
3. The messages between an MV and SP or a user and SP are encrypted with the session key. A timestamp is included in each message to ensure the message freshness and against replay attack.

- Security requirements is being satisfied:
  - Message Confidentiality: Encrypted with session key
  - Message Authentication, Integrity: signed by MAC
  - Message Freshness: timestamp

A Security Framework for MLS

- SP is a trustworthy party.
- Phase I: Initialization Phase
  - Session keys, MAC keys setup
- Phase II: MV/User Location Update Phase
  - Location Verification
- Phase III: Service Request Phase
  - Use transaction number or fake ID, instead of the MVs or users real information, to reduce the privacy exposure.

Phase I: Initialization between Service Provider and Mobile Vendor



Service Provider

Mobile Vendor

Get $Cert^{CA}_{SP}(KU_{SP}, KR_{SP})$ from CA. Create an entry for MV in DB and Reputation System.

Registration

… …

Get $Cert^{CA}_{MV}$ (KU_{MV}, KR_{MV}) from CA., and $Cert^{CA}_{SP}$ from SP

Registration

Verify $Cert^{CA}_{MV}$, save KU_{MV} in DB

$$Cert^{CA}_{MV}, E_{KU_{SP}}(ReqSI, E_{KR_{MV}}(ReqSI))$$

$$ReqSI = (ID_{MV}, t_{m_0}, SignIn)$$

Create session key K_{SM} and K^{mac}_{SM}, distribute to MV

$$Cert^{CA}_{SP}, E_{KU_{MV}}(SesKey, E_{KR_{SP}}(SesKey))$$

$$SesKey = (ID_{SP}, ID_{MV}, t_{S_0}, K_{SM}, K^{mac}_{SM})$$

Verify $Cert^{CA}_{SP}$, save K_{SM} and K^{mac}_{SM}

Sign in

ML Service using K_{SM} and K^{mac}_{SM}

Expires K_{SM} and K^{mac}_{SM},

$$E_{K_{SM}}(ReqSO, MAC_{K^{mac}_{SM}}(ReqSO))$$

$$ReqSO = (ID_{MV}, t_{m_n}, SignOut)$$

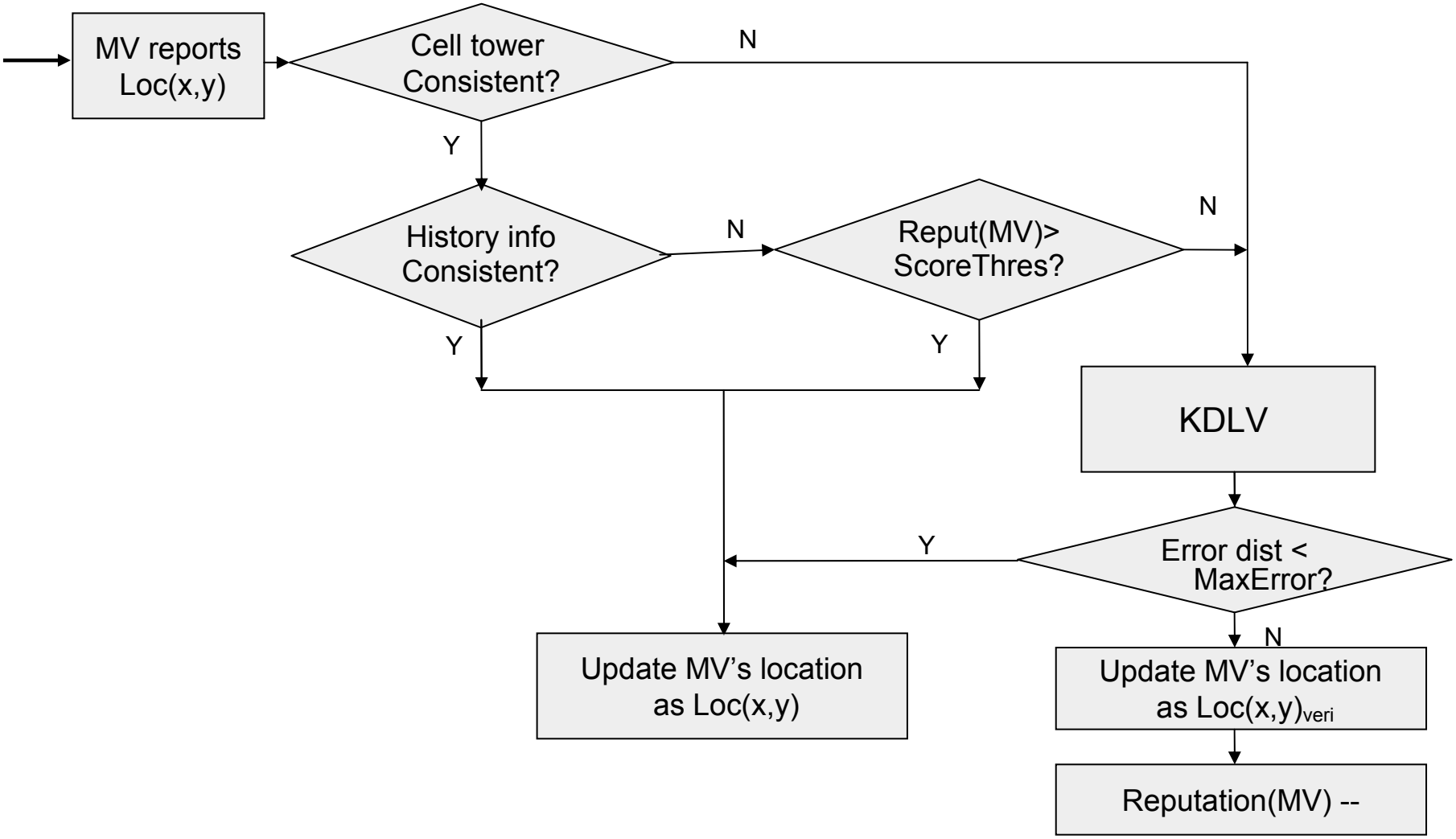
Data freshness,

Against reply attack,

Location consistency check

Sign out

Phase II: Location updating Procedure



Phase III: Service Request using Session key and MAC

Message Format:

$$\begin{cases} E_{K_{Session}}(Data, MAC_{K_{Session}^{MAC}}(Data)) \\ Data = (ID_{sender}, t_{m_i}, Msg) \end{cases}$$

$Msg1, U \rightarrow SP : ReqServ$

$Msg2, SP \rightarrow U : ReqLocation$

$Msg3, U \rightarrow SP : Loc_U(x, y)$

$Msg4, SP \rightarrow U : Info(MV_1), Info(MV_2), \ldots$

$Msg5, U \rightarrow SP : Req : MV_i, MWT$

$Msg6, SP \rightarrow MV_i : ReqServ, Loc_U, Req\#, MWT$

$Msg7, MV_i \rightarrow SP : AcceptReq, Req\#, EAT$

$Msg8, MV_i \rightarrow SP : NotAcceptReq, Req\#$

$Msg9, SP \rightarrow MV_i : GoServe, Req\#$

$Msg10, SP \rightarrow U : MV_i WillServe, EAT$

$Msg11, MV \rightarrow SP : ServiceEvaluation$

$Msg12, U \rightarrow SP : ServiceEvaluation$

MWT: Maximum waiting time

EAT: Estimated Arrival time

Summary

- Security Threats Analysis for Mobile Location-based Services
- Key Distribution based Location Verification (KDLV) method
  - Investigated the deployment requirement for KDLV.
- A security framework for MLS that properly combines cryptographic methods and location verification methods.

Thank you!

Investigate KDLV : k-N relationship

k- λ relationship

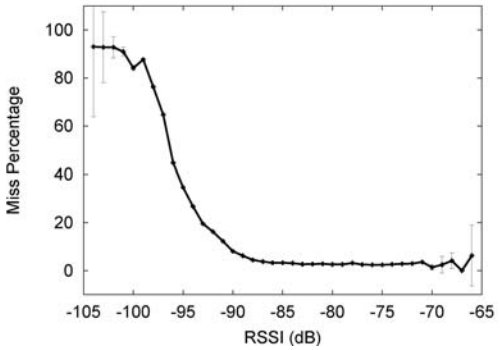
- ρ: the probability of receiving from a transmitter within distance d
- For a given ρ, the probability of receiving k keys from the n transmitters in A follows Binomial distribution: $q_{k,n} = \binom{n}{k} \rho^{k} (1 - \rho)^{n-k}$
- The probability of receiving at least k keys by the user, for a certain λ

$$p_k = \sum_{n=k}^{N} (p(N(A) = n) Q_{k,n}), \text{ where } Q_{k,n} = \sum_{j=k}^{n} q_{j,n}$$

λ-N relationship -- determines *d* from ρ

- Empirical data tested in typical environment gives us the relationship between ρ and P_{thre}.

ρ (%)	60	65	80	90	95
P_{thre}(dBm)	-95.63	-95	-93	-90.5	-89



- Using log-distance path loss model, $PL(d)[dBm] = P_0 - 10\gamma \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma$
- Then, obtain *d* from $P_T - PL(d) > P_{thre}$