Some of the work presented here was partially sponsored by NSF through grants 1314598, 1265886, and 1431244; by Motorola Solutions; and by the industry affiliates of the Broadband Wireless Access & Applications Center and the Wireless @ Virginia Tech group.

Security and Privacy Issues in Spectrum Access System (SAS)-Driven Spectrum Sharing

Jerry Park
(jungmin@vt.edu)

Dept. of Electrical & Computer Engineering
Virginia Tech

Oct 6, 2014

Wireless @ Virginia Tech

VirginiaTech Invent the Future

BWAC Broadband Wireless Access and Applications Center

Agenda

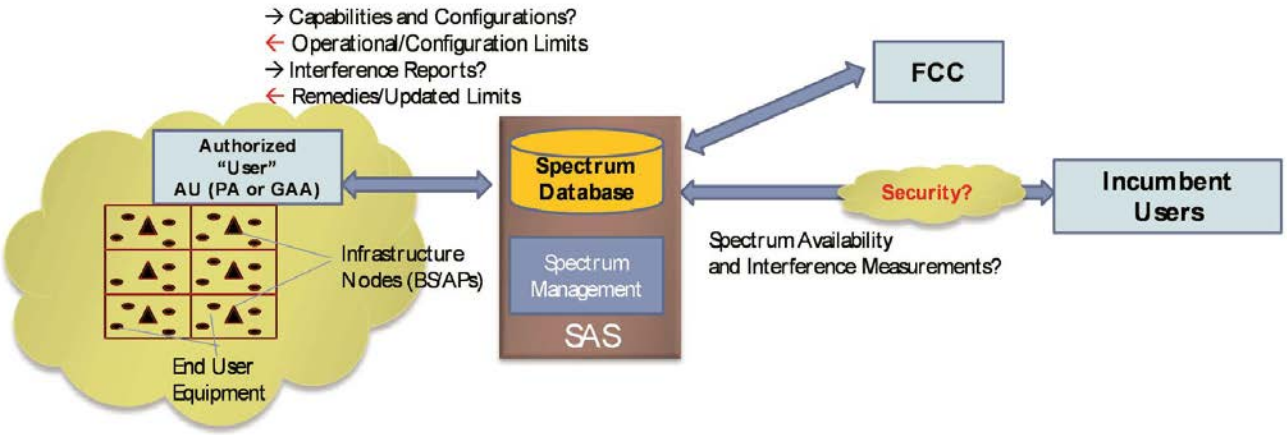
- Introduction to SAS and relevant security/privacy issues
- Threats to the primary user's (PU's) operational privacy (database inference attacks)
- Threats to the secondary user's (SU's) privacy
- Threats to the SAS database access protocol
- Enforcement approaches for countering rogue transmitters

Introduction to SAS and Relevant Security & Privacy Issues

J. Park, J. Reed, L. Beex, T.C. Clancy, Vireshwar Kumar, and Behnam Bahrak, "Security and Enforcement in Spectrum Sharing," *Proceedings of the IEEE*, Vol. 102, Issue 3, 2014, pp. 270-281.

Introduction to SAS

- The Presidential Memorandum, “Expanding America’s Leadership in Wireless Innovation”, released on 6/14/2013, directed the implementation of “policies for sharing with authorized non-federal parties of classified, sensitive, or proprietary data regarding assignments, utilization of spectrum, system configurations, business plans, and other information”.
- The Presidential Council of Advisors on Science and Technology (PCAST) released a report in July 2012 that advocated setting up Spectrum Access System (SAS) databases



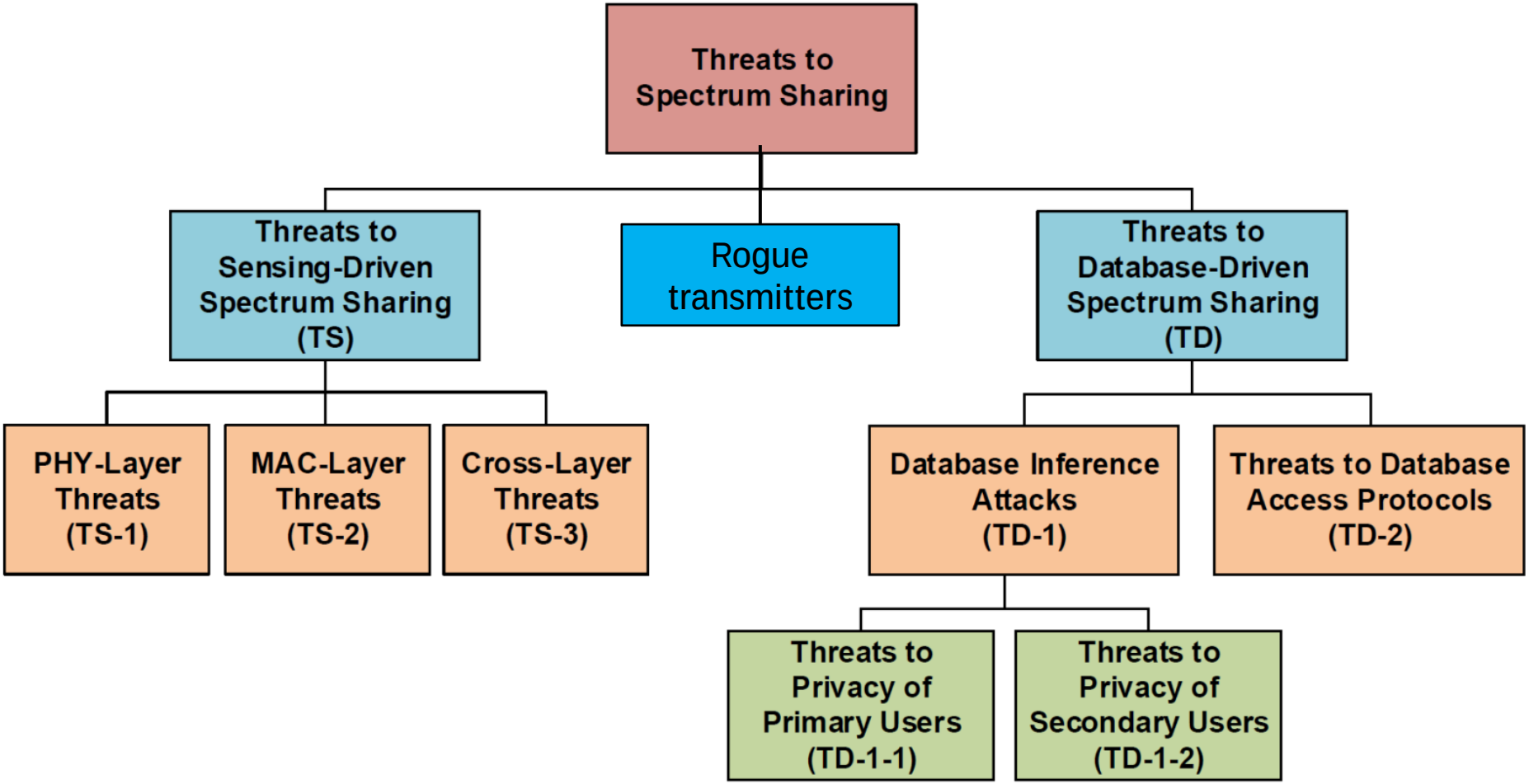
Introduction to SAS

- SAS can be considered a dynamic database system that...
  - Has a uniform interface analogous to the Internet's Domain Naming System (DNS), to provide federal information and access restrictions
  - Should employ a standard protocol to access the DB that supports interoperability among heterogeneous devices and databases (e.g., IETF PAWS (Protocol to Access White Space database))
  - Likely to consist of a number of logical and physical components that...
    - Process and respond to queries from registered SUs
    - Determine in real time channel availability based on PU spectrum utilization & protection zones, terrain profiles, SU info (from the queries), policy & regulations, sensing reports, etc.
    - Adjust the protection zone contours (when needed)
    - Carry out or support spectrum enforcement functionalities

Security in Spectrum Sharing

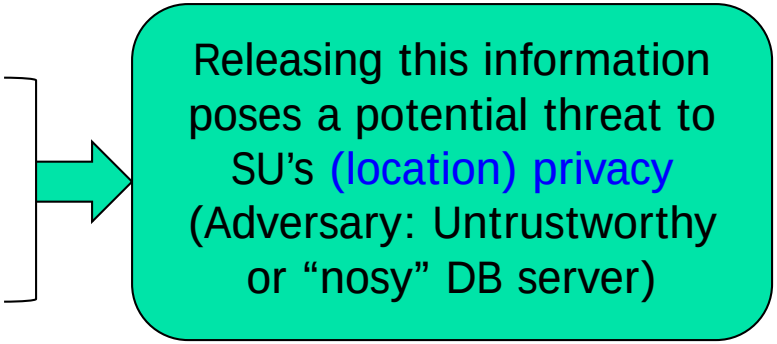
- When different stakeholders share a common resource, such as spectrum, security and enforcement become critical considerations that affect the welfare of all stakeholders.
- Threats to spectrum sharing often exploit the mechanisms which enable coexistence
  - viz, spectrum sensing and geolocation databases (GDB)

Taxonomy of Threats to Spectrum Sharing

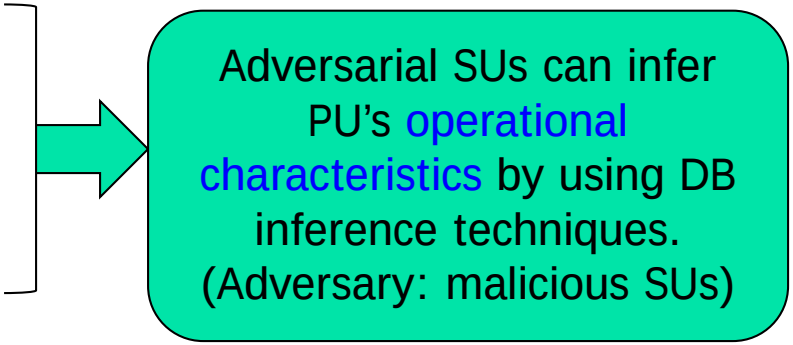


Threats to User Privacy

- Secondary users (SUs) query the DB to obtain spectrum availability information; a query includes:
  - SU's device identifier
  - SU's location & accuracy of that location
  - Antenna characteristics (type, height, etc.)



- GDB responds with a query response:
  - One or more whitespace (fallow) channels
  - Maximum allowed TX power
  - Time duration of allowed use
  - Possibly other info.



Threats to the DB Access Protocol

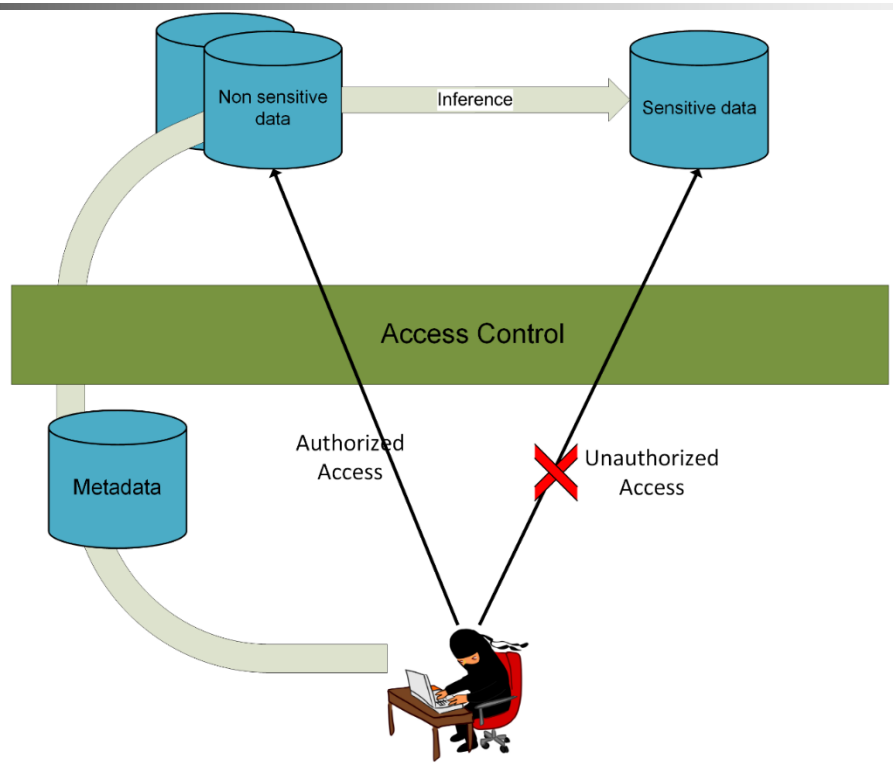
- DB access protocol: A standard protocol to access the DB that supports interoperability among heterogeneous devices and databases
- An attacker can target the following facets of a DB access protocol:
  - Source or data authentication
  - Data integrity
  - Availability of the DB server
- Examples:
  - Masquerade as another certified SU device, spoofed DB
  - Unauthorized modification of DB query replies
  - Denial of service (DoS) attacks against a DB server

Threats to the Primary User's Operational Privacy

B. Bahrak, S. Bhattarai, A. Ullah, J. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, April 2014.

A. Robertson and J. Molnar, "Spectrum database poisoning for operational security in policy-based spectrum operations," IEEE MILCOM, Nov. 2013.

Background: Database Inference Attacks



- Inference is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received
- Attacker uses a combination of data items (nonsensitive data + metadata) to infer data of a higher sensitivity

Background: Database Inference Attacks

- Inference detection is a very challenging problem and the subject of ongoing research
- In a relational DB, inference detection is a very difficult problem
  - In statistical DBs, progress has been made in devising inference detection techniques
- Two approaches for dealing with database inference:
  - Inference detection during database design:
    - Removes an inference channel by altering the DB structure or by changing the access control regime to prevent inference
  - Inference detection at query time:
    - Eliminate an inference channel violation during a query or series of queries by altering a query or denying it

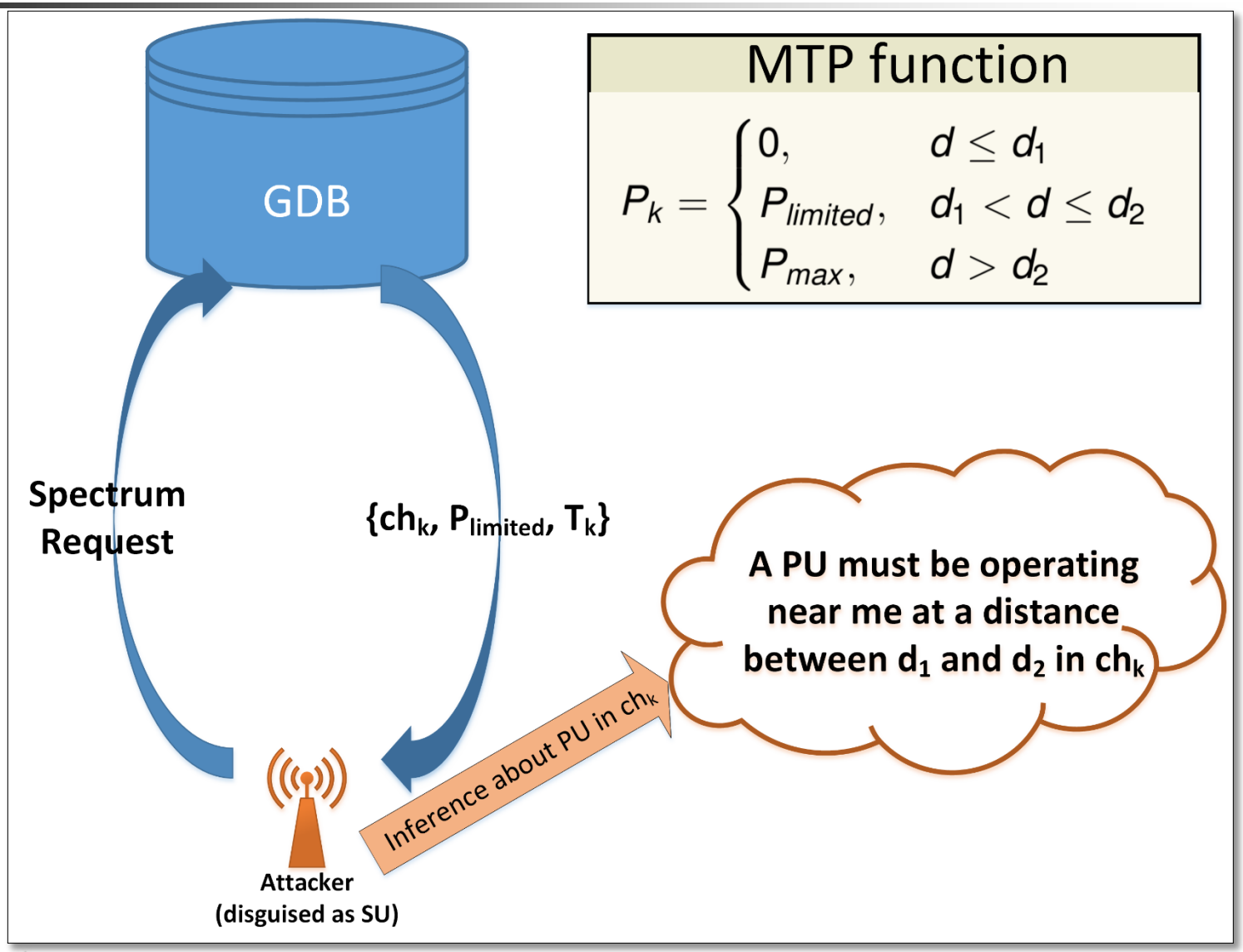
Traditional Databases Versus SAS

- Traditional databases
  - Inference attacks are thwarted by:
    - Splitting data into multiple tables and implementing access control for each table
    - Generating statistics from underlying probability distributions of data attributes, and then use them to perturb the data
- SAS
  - Access control cannot be applied
    - Spectrum availability information should be provided to all requesting (and registered) SU devices
  - Statistics cannot be used because:
    - SAS is not a statistical database; it does not publish aggregate information
    - SAS data items are based on individual database entries (e.g., nearest PU from the query location and its operational parameters)

Database Inference Attacks in SAS

- A serious concern when the PUs are nodes in a military or other type of Federal gov't network
- An attacker, through seemingly innocuous queries to the database, may be able to infer the operational characteristics of the PUs
  - Geolocation
  - Path of movement (of mobile PUs)
  - Transmission power
  - Receiver sensitivity or operating characteristics
  - Times of operation

Example: PU Location Inference Attack



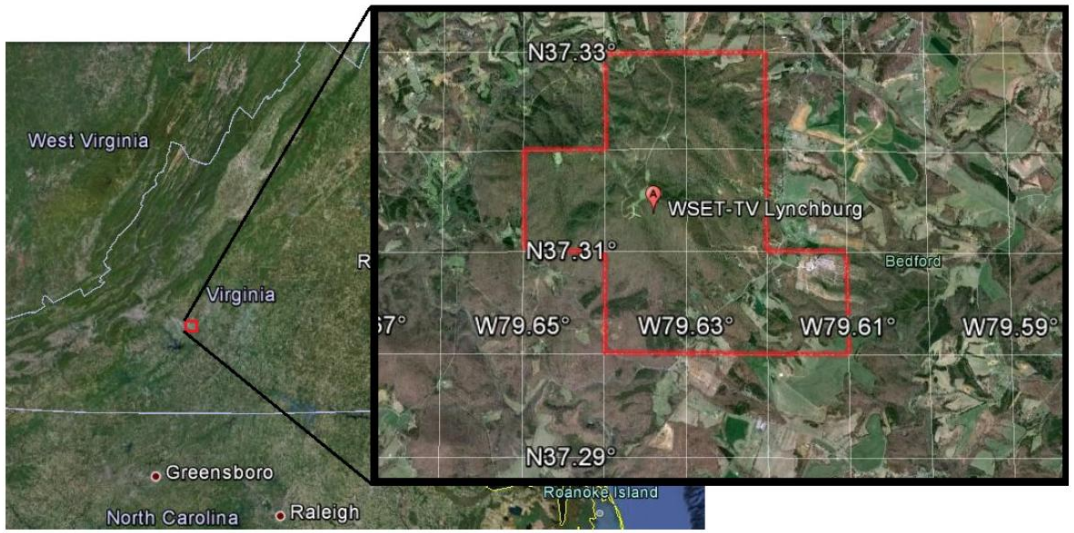
Example: PU Location Inference Attack

- Adversarial SUs can use Bayesian inference techniques to infer the location of stationary PUs using query responses

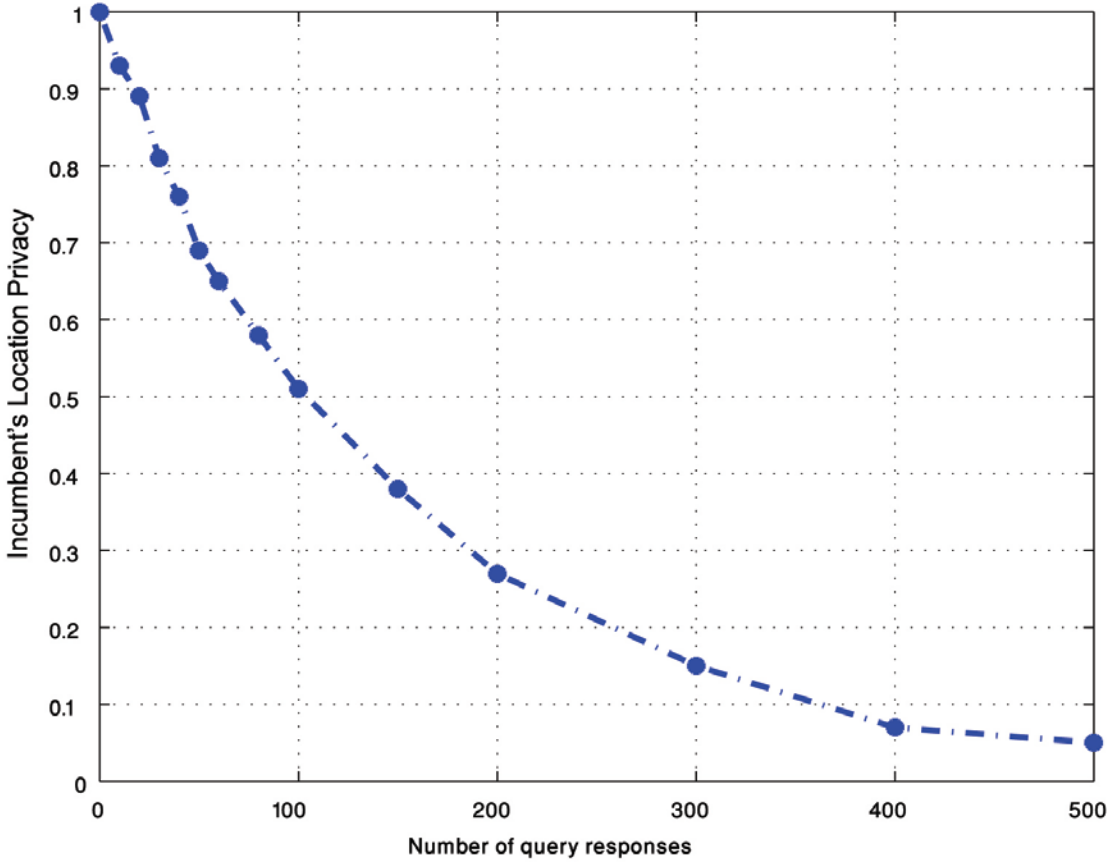
Algorithm 1 Stationary PU Location Inference Algorithm

Input: Sequence of queries $Q = \{q_1, q_2, \cdots\}$ and their corresponding responses $R = \{r_1, r_2, \cdots\}$.
Output: Location of PUs in the grid

```
Initialize p_ij^(k) values:
for all cells c(i,j) and channels k do
    p_ij^(k) = 1/2.
end for
while an inference has not occurred do
    Send query q_i = (ID_i, loc_i, A_i) to the database.
    Receive the list of available channels r_i = {(ch_k, P_k, t_k)}.
    for each channel k do
        if k is not in R then
            Compute distance d using the MTP function.
            Use d and location of the SU to find p-cells.
            Update p_ij^(k) values for the p-cells using equation 1.
            if p_ij^(k) > δ then
                an inference has occurred.
                return c(i,j) and k
            end if
        else if k is in R with a limited power then
            Compute distances d_1 and d_2 using the MTP function.
            Use d_1, d_2 and location of the SU, to find p-cells and
            e-cells.
            Update p_ij^(k) values for the p-cells using equation 1.
            if p_ij^(k) > δ then
                an inference has occurred.
                return c(i,j) and k
            end if
            Put p_ij^(k) = 0 for the e-cells.
        else if k is in R with maximum possible power then
            Compute distance d using the MTP function.
            Use d and location of the SU to find e-cells.
            Put p_ij^(k) = 0 for the e-cells.
        end if
    end for
end while
```



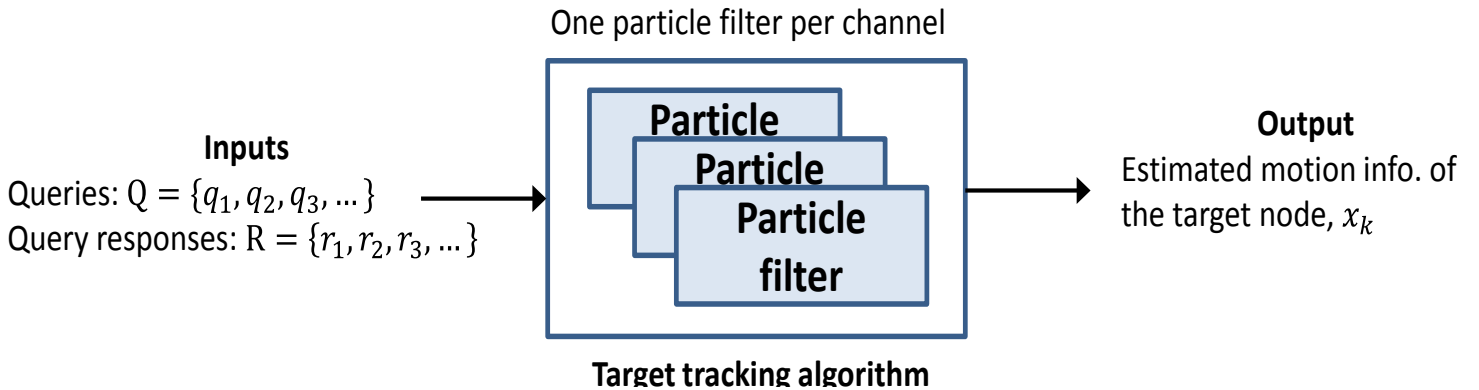
Example: PU Location Inference Attack

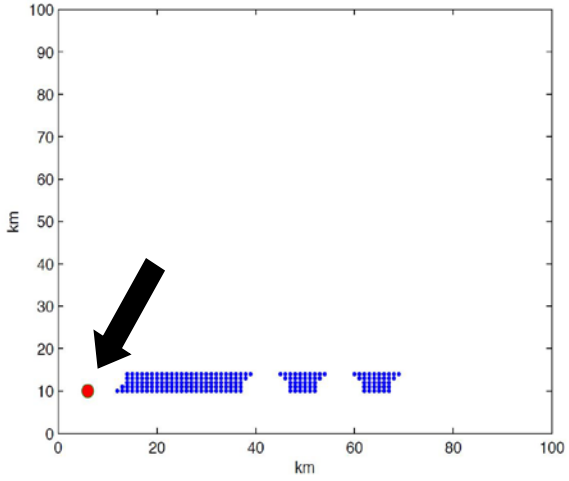


Metric for location privacy: *incorrectness*
Incorrectness: Expected distance between the location inferred by the attacker and the PU's true location .

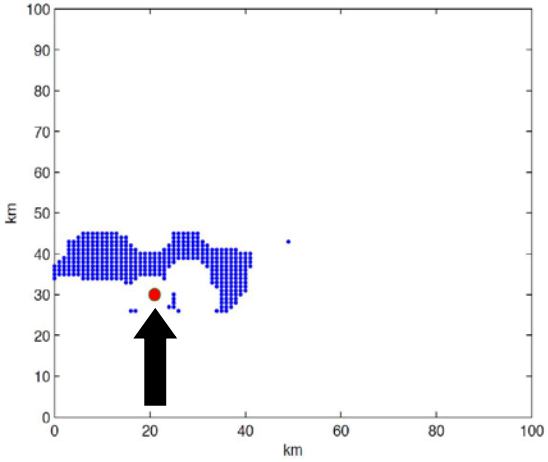
Example: Tracking PU's Path of Movement

- Adversarial SUs can use particle filters (recursive Bayesian estimation) to infer and track the movement of mobile PUs

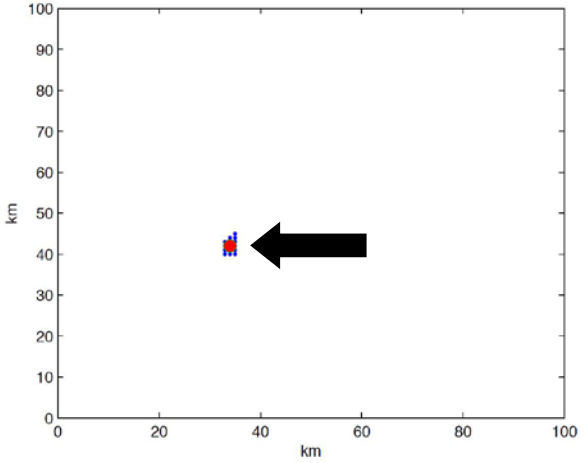




(a) After 15 iterations



(b) After 50 iterations

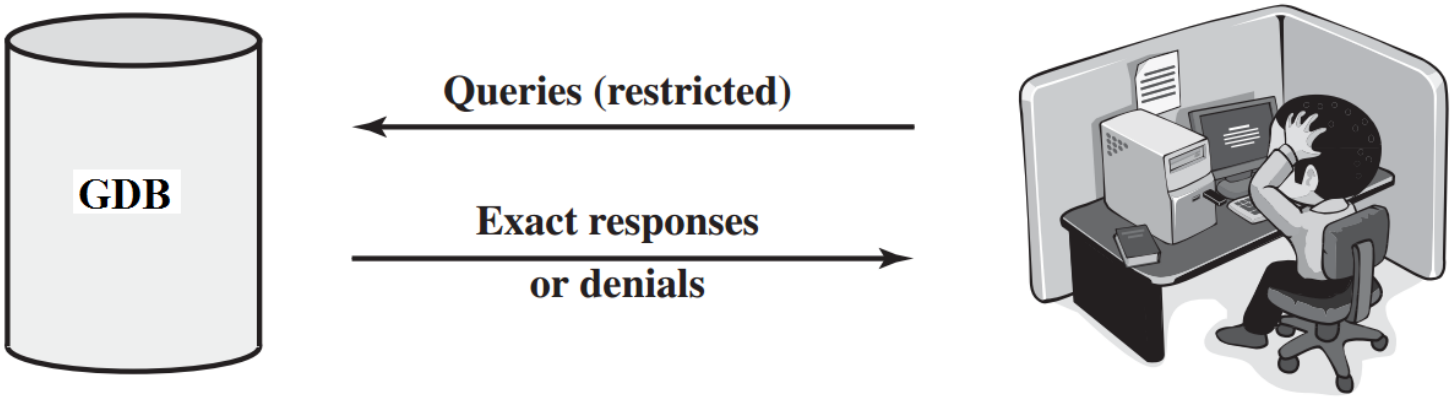


(c) After 75 iterations

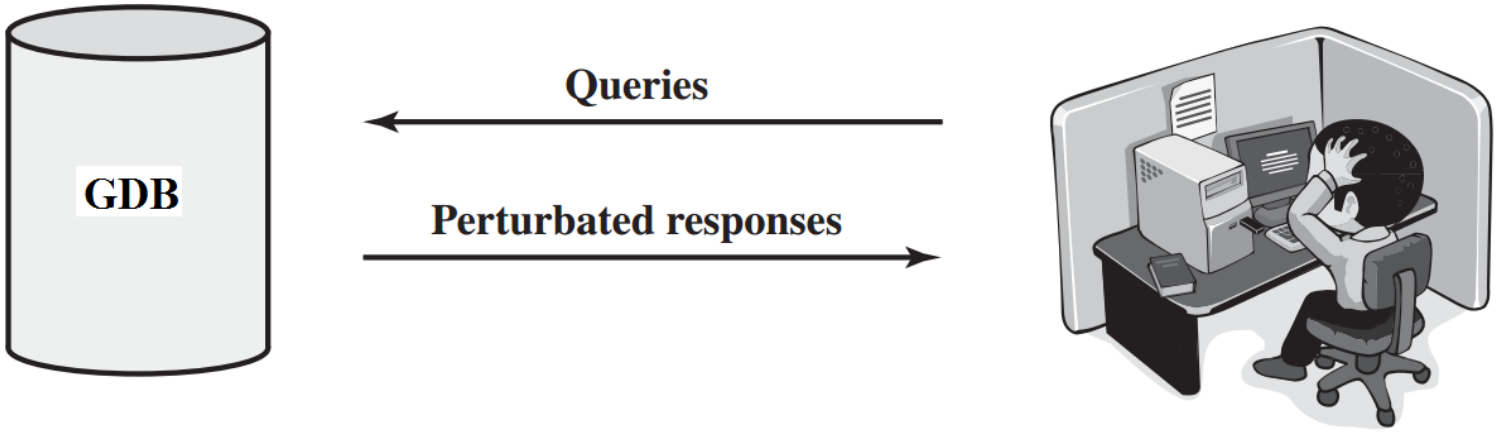
Particles tracking a target's movement.

Database Privacy Preserving Techniques

Query set restriction



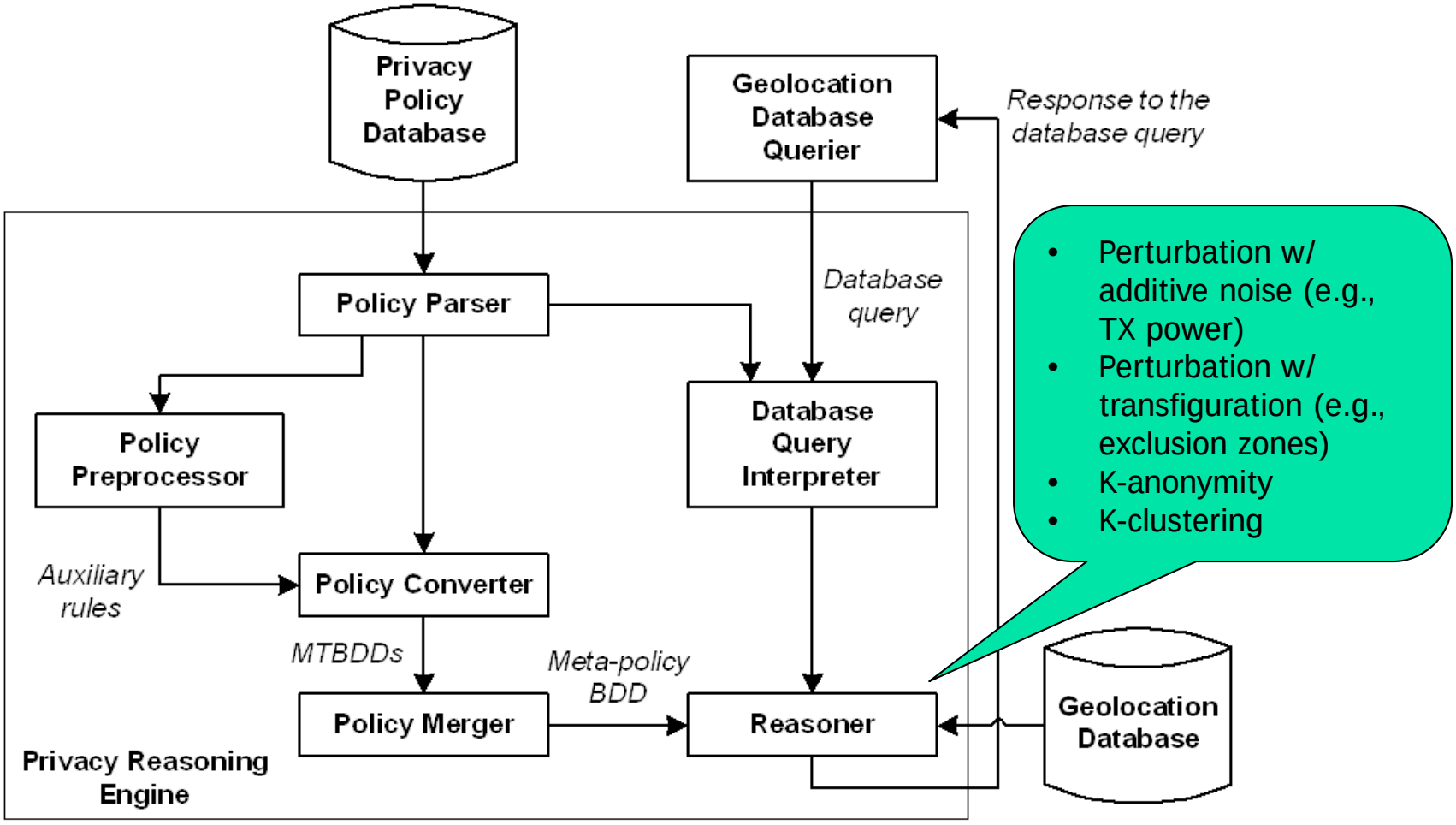
Output perturbation



Output Perturbation Techniques for SAS

- Location privacy
  - Perturbation w/ noise (E.g., SU transmit power)
  - Perturbation w/ transfiguration (E.g., Exclusion zones)
  - k-anonymity
  - k-clustering
  - Add dummy primary users
- Times of operation privacy
  - Buffer times slots
  - k-anonymity

Obfuscated Spectrum Database



Architecture of an obfuscated database

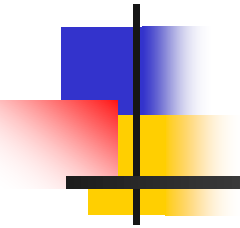
Threats to the Secondary User's Privacy

Privacy Threats to the Secondary User

- SU includes its identity, location, antenna parameters, etc. in a database query
- Potential privacy issue if the (commercial) SAS is not trustworthy or has been compromised
- An attacker may obtain/infer SU's info or his/her spectrum usage habits, including:
  - Identity
  - Location
  - Device type (e.g., antenna parameters, maximum TX power)
  - Times of operation (it is correlated to the query times)
  - Mobility information
  - Possibly other information

Possible Privacy Preserving Techniques

- Two-way authentication between SAS and SU
  - Enables both the SAS and SU to authenticate each other
- Require SUs to send only those parameters that are needed for computing spectrum availability
- Commercial SAS uses partially homomorphic encryption techniques to process queries
  - Spectrum availability information (provided by the Federal SAS) stored in encrypted form
  - A SU sends a query with encrypted parameters to a commercial SAS
  - Commercial SAS performs computations on encrypted data, and responds to the query with spectrum availability information



Threats to the SAS Access Protocol

Threats to SAS Access Protocol: Introduction

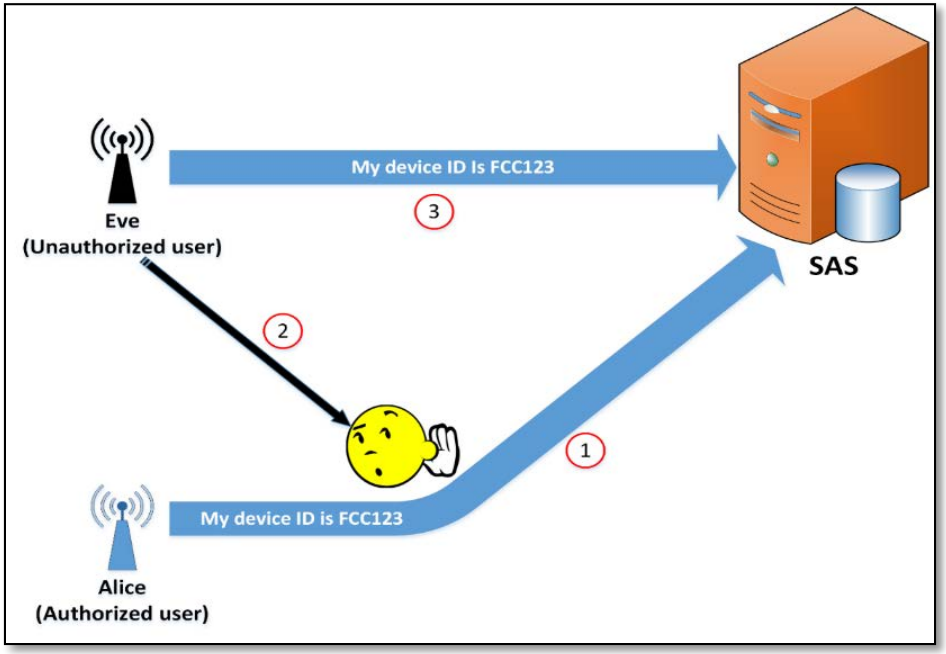
- SAS access mechanism is expected to be similar to the one used for accessing a DNS server
  - Some of the attacks that can be launched against a DNS server can also be launched against the SAS
- An attacker can target the following facets of a DB access protocol:
  - Source or data authentication
  - Data integrity
  - Availability of the DB server
- Attacks against the SAS access protocol can impact both the PUs and SUs
  - e.g., SUs causing interference to the PUs

Threats to SAS Access Protocol: Introduction

- Internet Engineering Task Force (IETF) and others are studying security concerns specific to spectrum DB access protocols
  - E.g., Protocol to Access White Space database (PAWS)
- In general, three major classes of threats to DB access:
  - Loss of confidentiality
    - Protection of data from improper disclosure
  - Loss of integrity
    - Information should be protected from improper modification
  - Loss of availability
    - Making data available to a legitimate user with access privileges

Masquerade Attack

- Illegitimate user masquerades as a valid device
  - Without suitable protection mechanisms, devices can listen to registration exchanges, and later register with the database by claiming the identity of another device.
  - Multiple malicious SUs query the SAS from near SU's location resulting in no white space available for the legitimate SUs



SAS Pharming and SAS Data Poisoning

- SAS pharming
  - Redirect a legitimate SAS's traffic to another, bogus server
  - Pharming can be conducted by exploiting vulnerabilities in SAS server software (e.g., DNS cache poisoning → SAS cache poisoning)
  - Bogus SAS is under the attacker's control
  - Can be used to cause interference to PUs
  - Bogus SAS may decline spectrum queries from legitimate SUs, and thus cause a denial of service attack
- SAS (Data) poisoning
  - Maliciously altering the contents of the SAS
  - SAS provides false white space information to the SUs

Modification of the Queries & Query Responses

- Modifying or jamming a DB query
  - An attacker modifies the SU's query before it reaches the database
  - Database responds to a modified query
  - Response might be unusable by the SU
- Modifying or jamming a DB query response
  - An attacker intercepts the database response and modifies it before it reaches the SU
  - When a SU uses the modified response, it may result in interference to the PUs

DoS or DDoS Attacks against the SAS

- Overwhelm the SAS with a large number of bogus queries
- Attacker may bombard the SAS with bogus queries from a large number of "zombie" SU queriers → distributed denial of service (DDoS) attacks
- Makes the SAS irresponsive to legitimate queries from other SUs
- DDoS tools are readily available
  - Extensive expertise not needed to launch sophisticated attacks
  - Tools available to "script kiddies": Trinoo, Tribe Flood Network (TFN), Stacheldraht, Shaft, TFN2K, Trinity

Countermeasures against the SAS Access Protocol Threats

- Filtering the requests that match the attack signature
  - Might lead to an immediate DoS to both attacker and the legitimate clients if not carefully designed
- Two way encrypted authentication between the SAS and the SU (querier)
  - Thwarts masquerade and database spoofing attacks
  - E.g., DNS-SEC uses one way authentication which ensures that the response originates from a legitimate server. Unfortunately, DNS-SEC does not ensure authentication of the requestor
- Integrity protection
  - Use of cryptography-based integrity protection mechanisms (e.g., message authentication codes)
  - Thwarts unauthorized modification of spectrum query/response
  - Thwarts unauthorized modification of the DB contents

Countermeasures against the SAS Access Protocol Threats

- Maintaining redundancy (multiple SAS)
  - Redundancy of spectrum availability information helps the SAS withstand DDoS attacks
    - E.g., 13 root DNS servers
  - DNS root server attack in Oct 2007. Redundancy in the DNS root servers prevented the attacker from crippling the Internet
- Improve stability by spreading the load of attacks
  - Anycast: It allows a number of servers in different places to act as if they are in the same place.
    - Multiple servers can support a root server to distribute the load
- Requiring SU registration and registration acknowledgement

Enforcement Approaches against Rogue Transmitters

V. Kumar, J. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," 2014 ACM Conference on Computer and Communications Security (CCS), Arizona, USA, Nov. 2014.

J. Park, J. Reed, L. Beex, T.C. Clancy, Vireshwar Kumar, and Behnam Bahrak, "Security and Enforcement in Spectrum Sharing (invited paper)," Proceedings of the IEEE, Vol. 102, Issue 3, 2014, pp. 270-281.

V. Kumar, J. Park, T. C. Clancy, and K. Bian, "PHY-Layer authentication by introducing controlled inter symbol interference," IEEE Conference on Communications and Network Security (CNS), Washington, D.C., Oct., 2013.

B. Bahrak, J. Park, and H. Wu, "Ontology-based spectrum access policies for policy-based cognitive radios," IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Oct. 2012.

Two Enforcement Approaches

- Database cannot enforce, through the protocol, that a client device uses only the spectrum it was authorized to use
- Devices can put energy in the air and cause interference without asking the database
- Two approaches for enforcing spectrum rules:
  - Ex ante (preventive) approach
  - Ex post (punitive) approach

Ex Ante (Preventive) Approach

- Mechanisms and techniques for preventing non-compliant transmissions
  - Mechanisms for “spectrum access control”
- Examples include:
  - exclusion/protection zones
  - policy-based radios (i.e., radio w/ a policy reasoner)
  - secure radio middleware
  - tamper resistance techniques
  - radio integrity assessment techniques
  - hardware-based compliance modules
- Ex ante enforcement reduces the cost associated with deploying ex-post enforcement measures

Ex Post (Punitive) Approach

- Remediate malicious or selfish behavior after a harmful interference event has occurred
- Ex post approaches include:
  - enforcement sensor networks
  - schemes for uniquely identifying rogue transmitters (e.g., PHY-layer authentication)
  - localization of non-compliant transmitters
  - adjudication procedures for non-compliant transmitters
    - Revocation of spectrum access rights
    - Economic penalties
- In general, ex post measures are expensive to employ

Privacy Implications of Ex Post Enforcement

- Ex post approaches may rely on schemes for uniquely identifying rogue transmitters (e.g., PHY-layer authentication)
- Transmitter authentication at the PHY-layer is one approach
- However, transmitting a SU's identity over the air poses thorny privacy issues
- Trade-off between SU privacy and ex post enforcement

Thank you

If you have questions, please email them to me

jungmin@vt.edu

For more details, visit

http://www.arias.ece.vt.edu/