Security and Data Reliability Measures for a Distributed, Noisy, and Potentially Adversarial Sensor Network

Alex Orailoğlu, Nickolai Verchok, Elbruz Ozen

UC San Diego
JACOBS SCHOOL OF ENGINEERING
Computer Science and Engineering

NSF 1739684

Security: Threats and Countermeasures

As the goal of the system is the detection of and response to a bomb-carrying adversary, **security** and **reliability of data** are of utmost importance. Our threat model assumes that an adversary will be motivated to thwart detection by **modifying node messages**, generating **false signals** both on-site and through remote injections of custom packets, and entirely disabling network components via **DDoS**. We are also assuming more subtle attacks on node **privacy** (location & timestamp data). The table summarizes our proposed countermeasures.

Threats for:	Countermeasures
• Integrity • Authenticity (Node Legitimacy) • Node Data Privacy	Cryptography
• System Reliability	Sensor Signal Consensus
• System Availability	DoS Resilience
• Authenticity (Node Physical Presence)	Location Validation

Cryptography: Sensor IDs & Encryption

Sensor IDs
- 2^{30} (10^9) uniformly-distributed 128-bit values
- 2^{98} invalid per 1 valid ID (10^6 years at 10 petaflops)
- Sensor IDs **are separate from physical sensors**
- Users provide **personal identification** to request a Sensor ID
- System accumulates requests then **distributes anonymously**

Encryption
- Node messages encrypted with Buffer public keys; signed with Node SID
- HQ messages encrypted with Node SID; signed with HQ private key

Reliability: Signal Consensus

Likelihood Decision Framework
- Probability model: **P(** ***sensor reading* | *distance from bomb, bomb potency*** **)**
- **Joint likelihood** for readings evaluated for all possible locations & potencies
- If *worst case* sufficiently greater than false-positive likelihood, **confirm threat**

Discrete Search
- Search space is **discretized to 4500 values** (9x10x10 locations, 5 potencies)

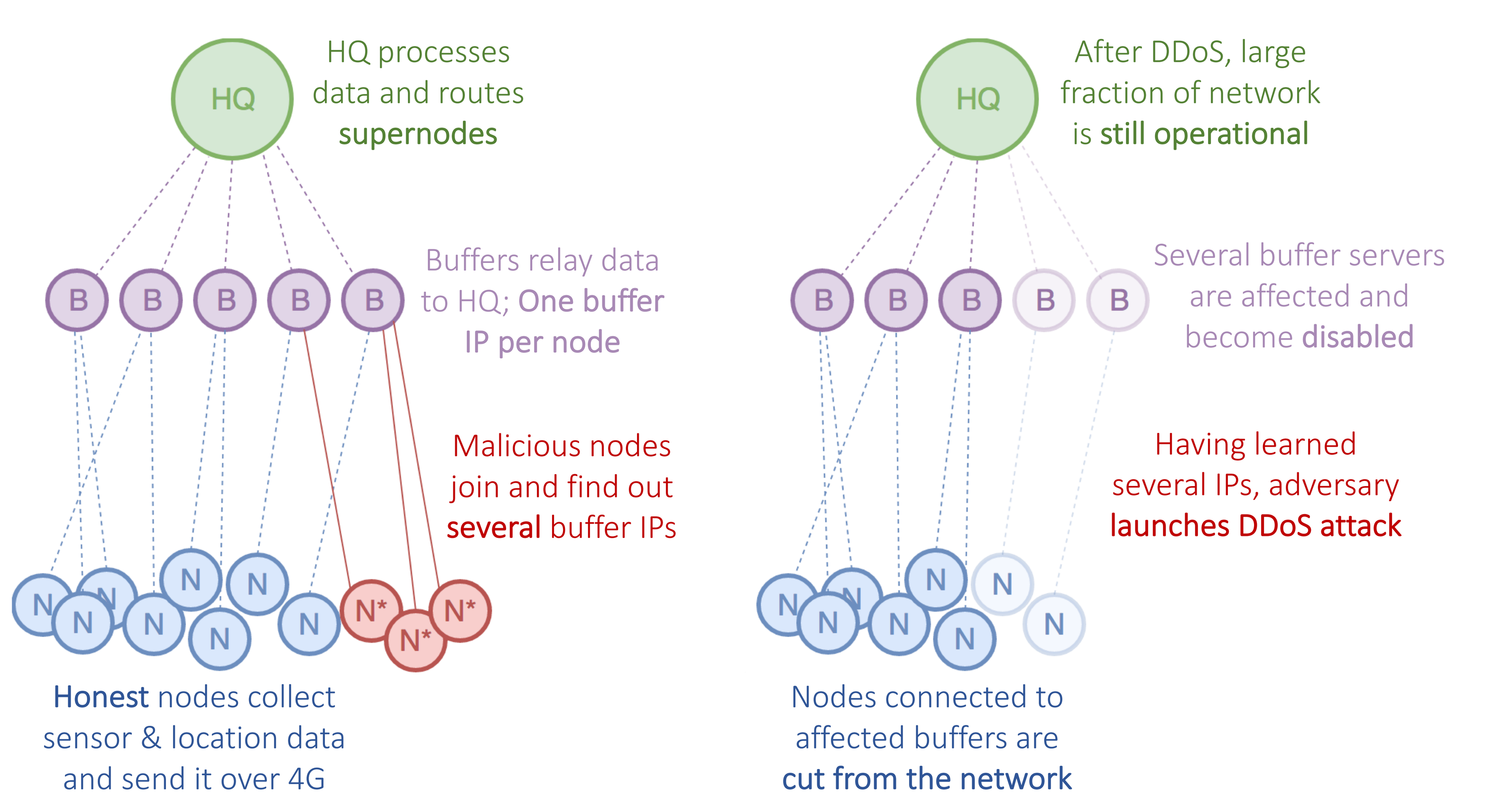
The decision is given by choosing a threshold P(T) and the equation:

$$P(T|S) > P(NT|S) \quad \Leftrightarrow \quad P(T) > \frac{P(S|NT)}{P(S|T)+P(S|NT)} \quad \text{where} \quad P(S|T) = \max_{1 \le i \le 4500}\left(\prod P(S_j|T = t_i)\right)$$

Availability: DoS Resilience

Threat Scenario
- Adversary wants to disable *most* of the network with a **DDoS attack**
- Adversary **has some valid SIDs** but **does not know any Buffer/HQ IPs**
- Adversary **slowly learns** IPs by joining with every SID

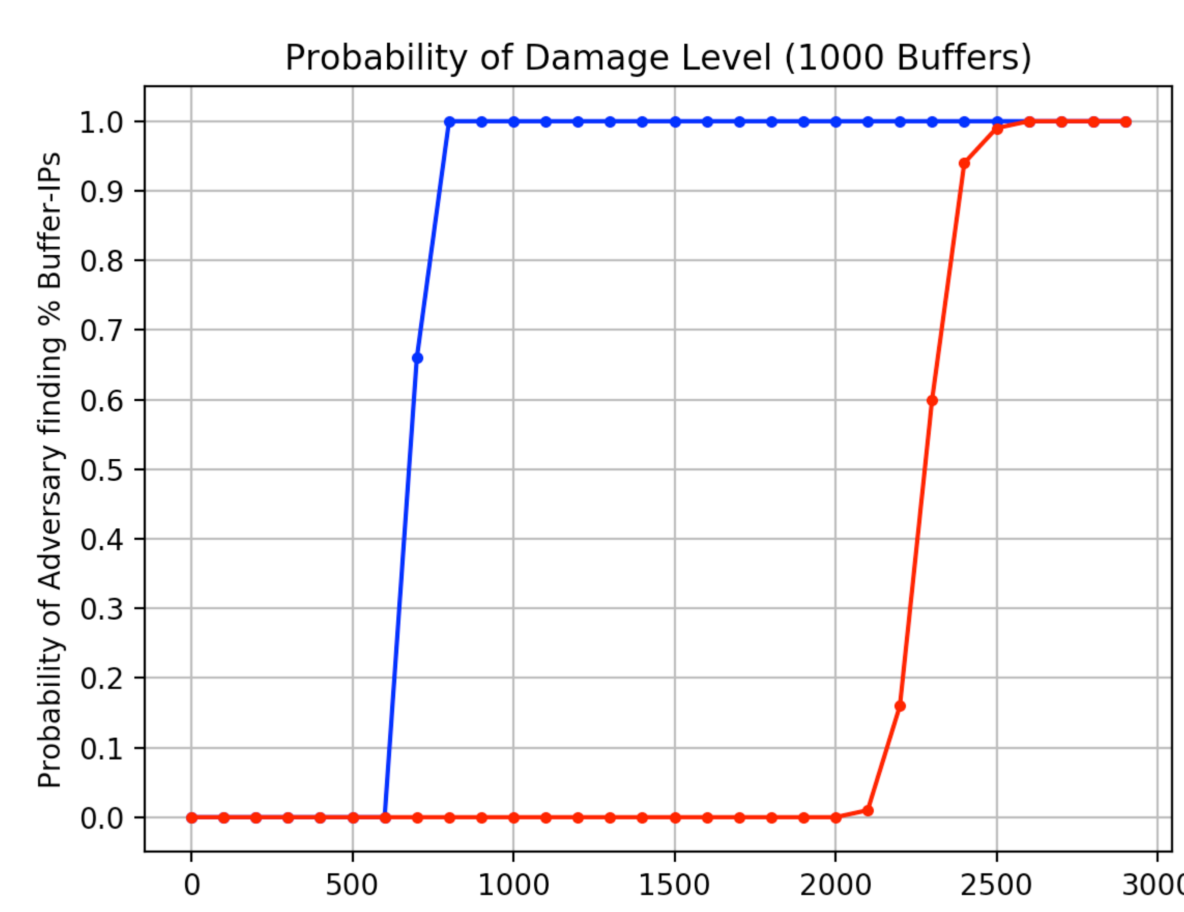
Countermeasure: Buffer Server Infrastructure



Countermeasure: Authentication Authority
- Separate server; initial communication point for **new nodes**
- Randomly **assigns (reveals) a single Buffer IP** to a valid Sensor ID
- Itself susceptible to DoS but *only new nodes affected*

Resilience Analysis

Monte-Carlo simulation of the probability of the adversary learning more than 50% and more than 90% of 1000 Buffer IPs for a given number of Sensor IDs at their disposal.

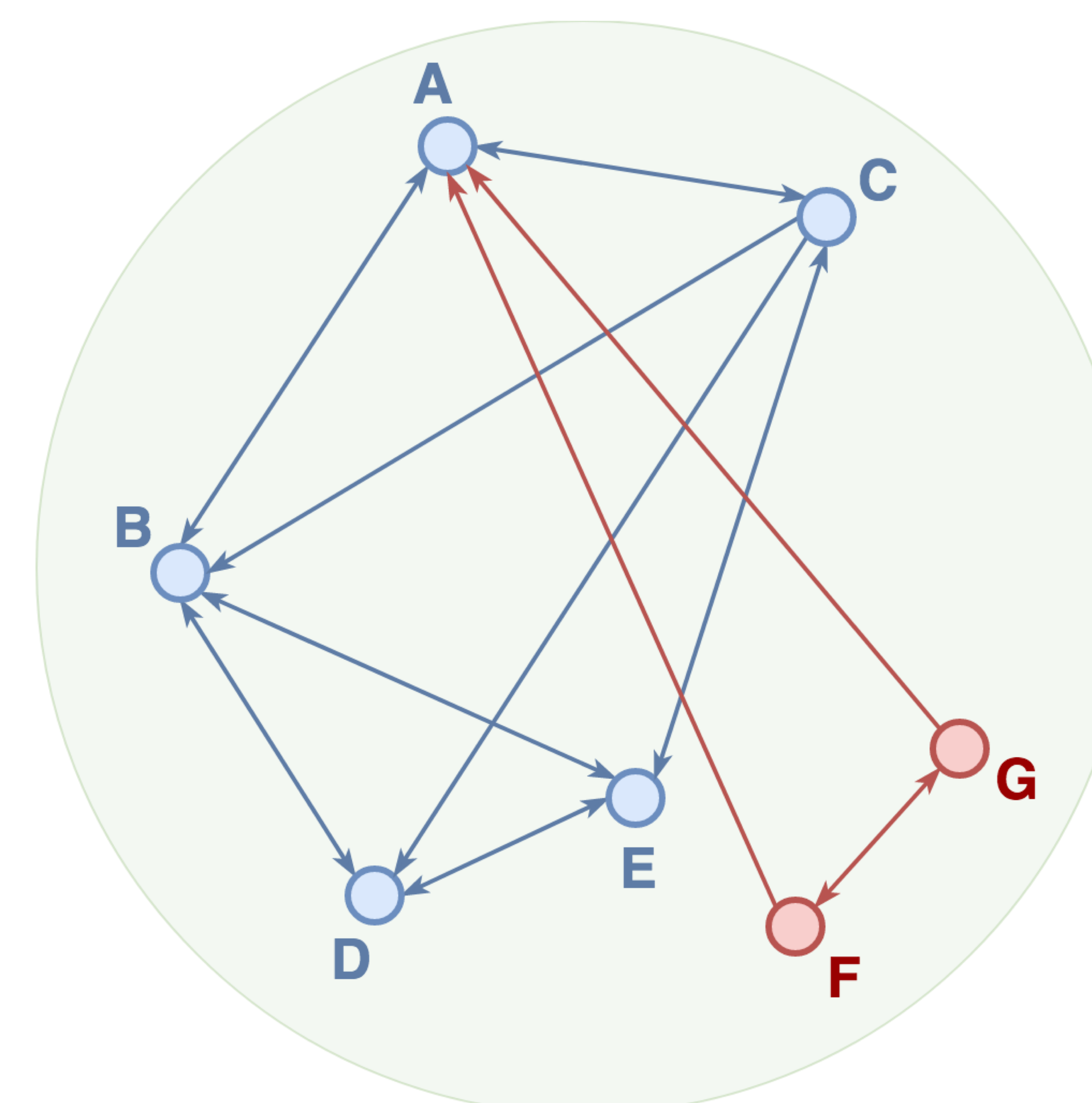


Adversary needs 700+ Sensor IDs to learn 500+ unique IPs; **2100+ to learn 900+** (data across 10,000 trials). Buffer infrastructure distributes DoS damage; **if SIDs are hard to obtain, then DoS is greatly hindered.**

Authenticity: Location Validation

Threat Scenario
- Adversary wants to **overpower Signal Consensus**
- Adversary can **spoof fake messages remotely** to *forge* nodes

Countermeasure
- Distribute **secret TAGs to nodes**
- Nodes **broadcast** TAGs via WiFi Direct
- Nodes tell HQ which TAGs they saw
- HQ performs a robust **statistical analysis**
- **Forged nodes are identifiable** as they:
  1) *cannot be seen by honest nodes*
  2) *cannot perfectly imitate location-credible data*



Nodes **G and F** will be **deemed suspicious** as they:
- are not seen by any other nodes except themselves
- see A but not D & E, which are closer

Achievements
- O(log(n)) algorithm that ensures full connectivity
- Simulation environment

Second Year Plan

- **Integrate security measures** into the simulator developed by other group members.
- **Extend the Signal Consensus** framework to:
  - search over possible bomber paths using recent data
  - incorporate data of individual node false-positive rates