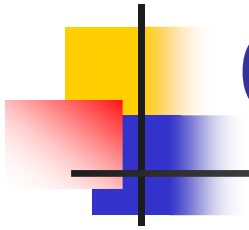
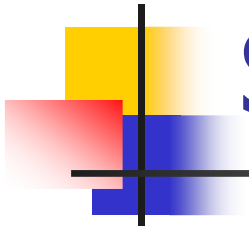
Secure Data Aggregation in Wireless Sensor Networks: A Survey

Hani Alzaid, Ernest Foo and
Juan Gonzalez Neito
Information Security Institute
Queensland University of Technology



Overview

- Background
- Attacks
- Existing Schemes
- Requirements
- Scheme Classification
- Adversaries

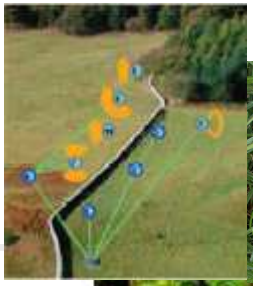


Sensor Networks

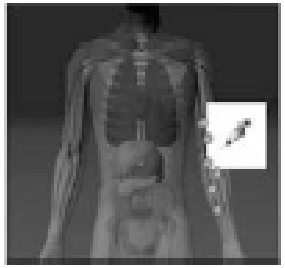
- Distributed network of wireless nodes that monitor the environment or other systems.
- Deployed in large numbers
- Nodes have limited battery life
- Nodes have low computational power
- Nodes have small data storage

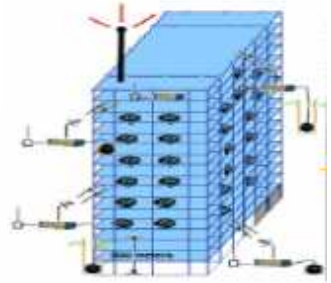
Sensor Networks

- Civil structural monitoring
- Habitat/ecosystem monitoring
- Environmental monitoring
- Smart homes
- Chemical Detection
- Traffic/Vehicle Monitoring
- Human Health Monitoring
- Homeland Security



Ecosystems, Biocomplexity





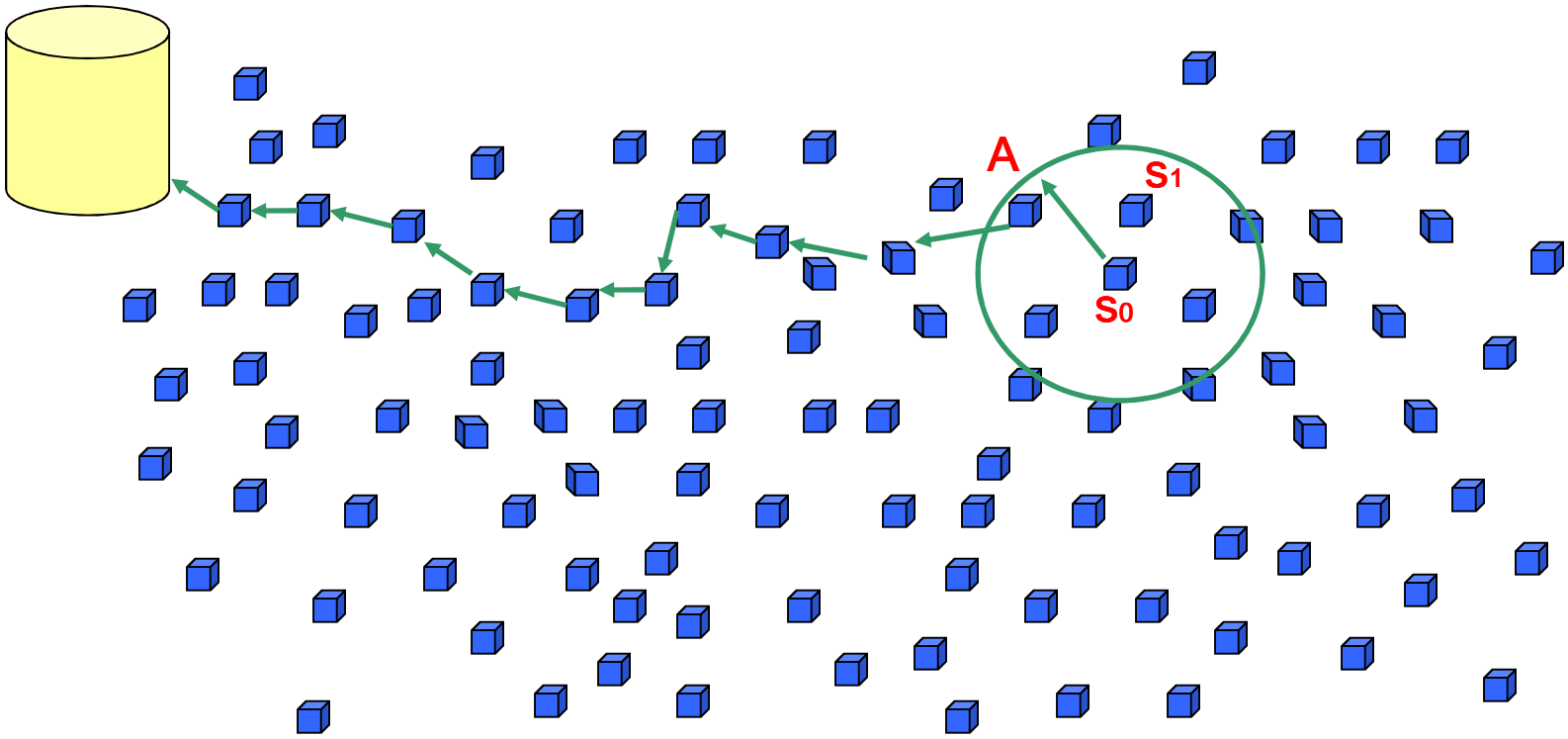
Asset Management

Manufacturing

Condition-Based Maintenance

Sensor Networks

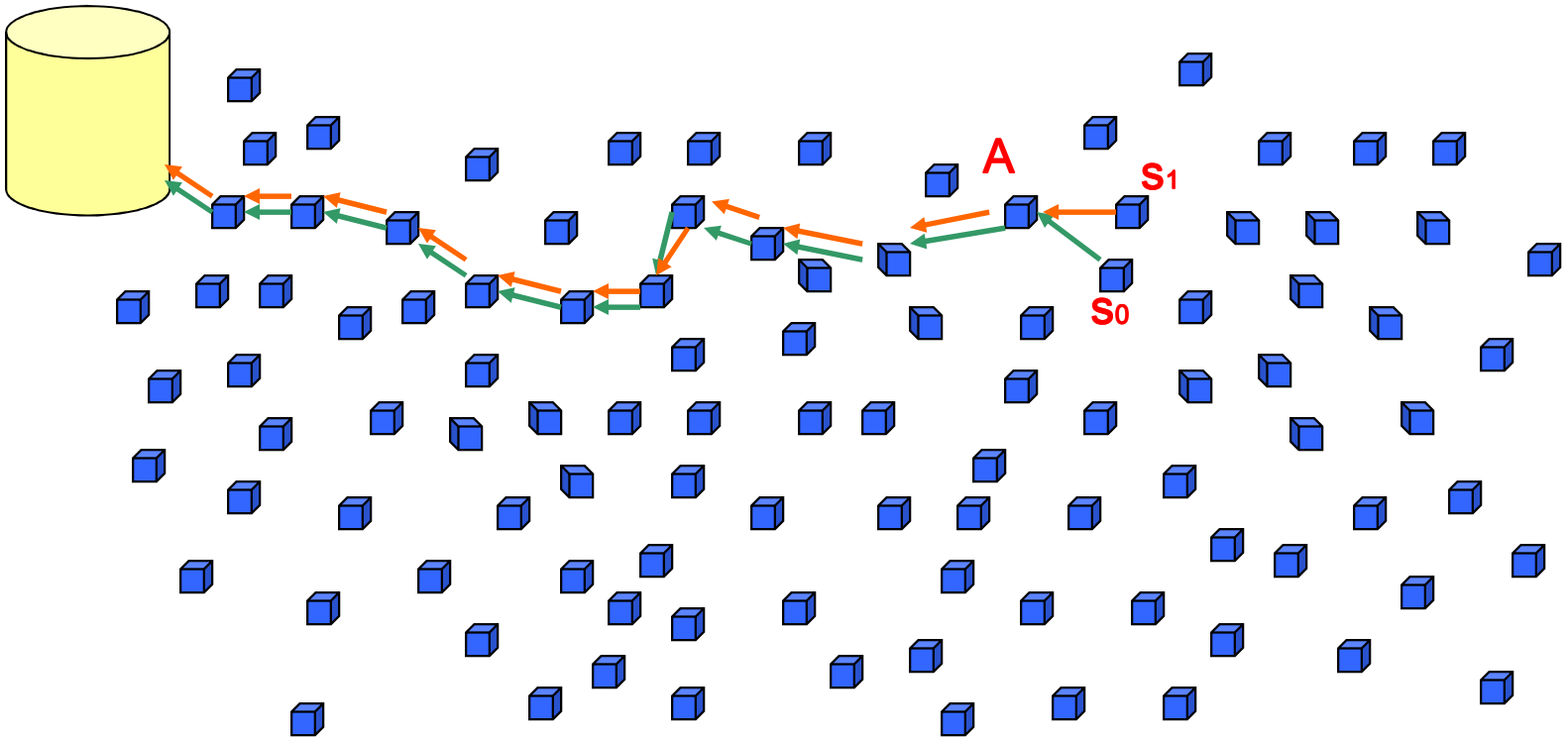
Base station



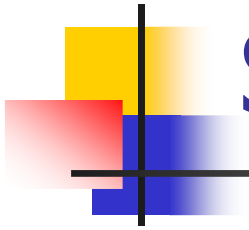
Thousands of small devices with sensors communicating wirelessly

Sensor Networks

Base station



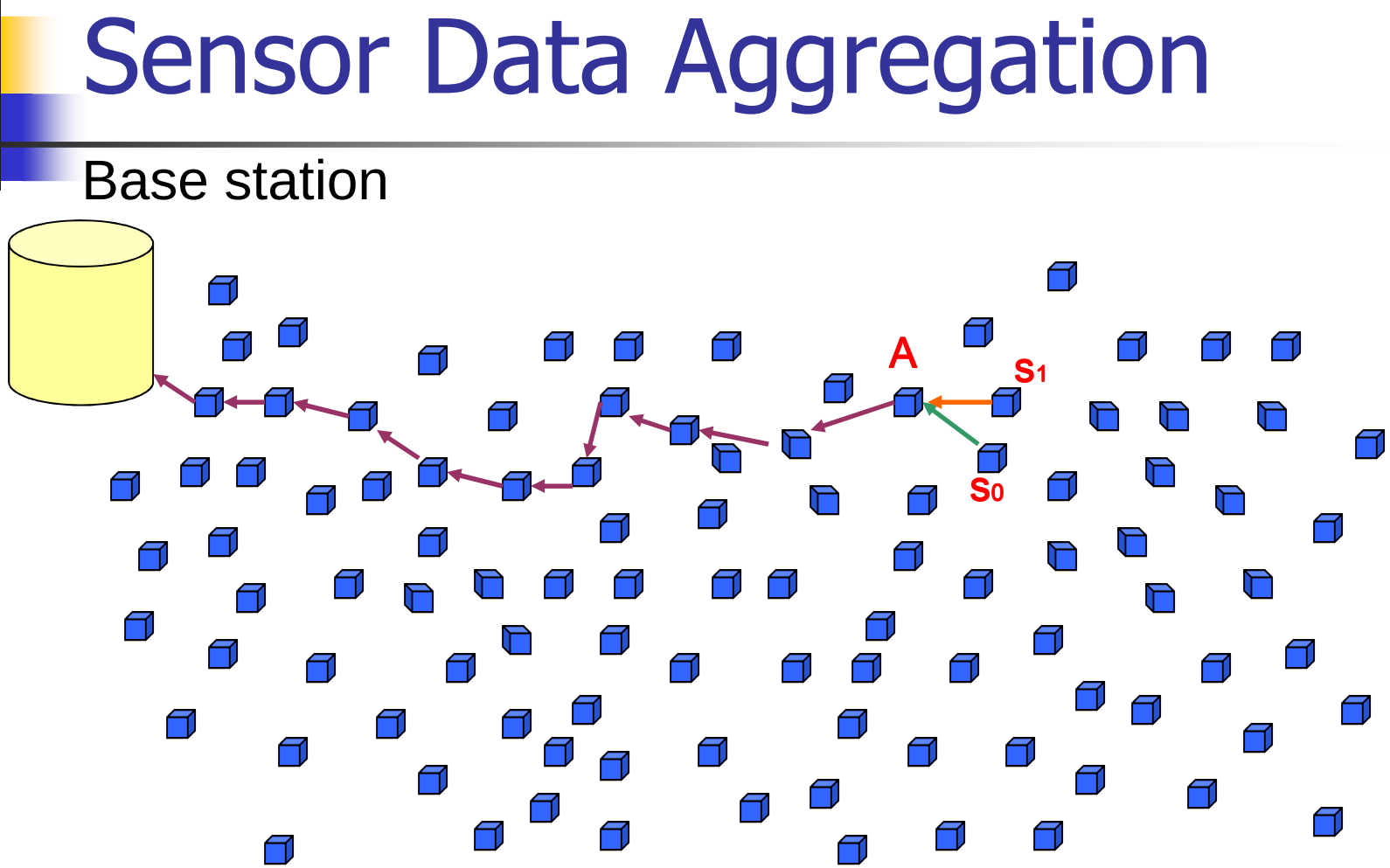
Transmitting each message all the way to the base station wastes resources.



Sensor Data Aggregation

- Approximation of the sensor readings although a limited number of nodes are compromised.
- Ability to reduce the size of the data transmitted through the network.
- Provide accurate aggregation results without exhausting the network.

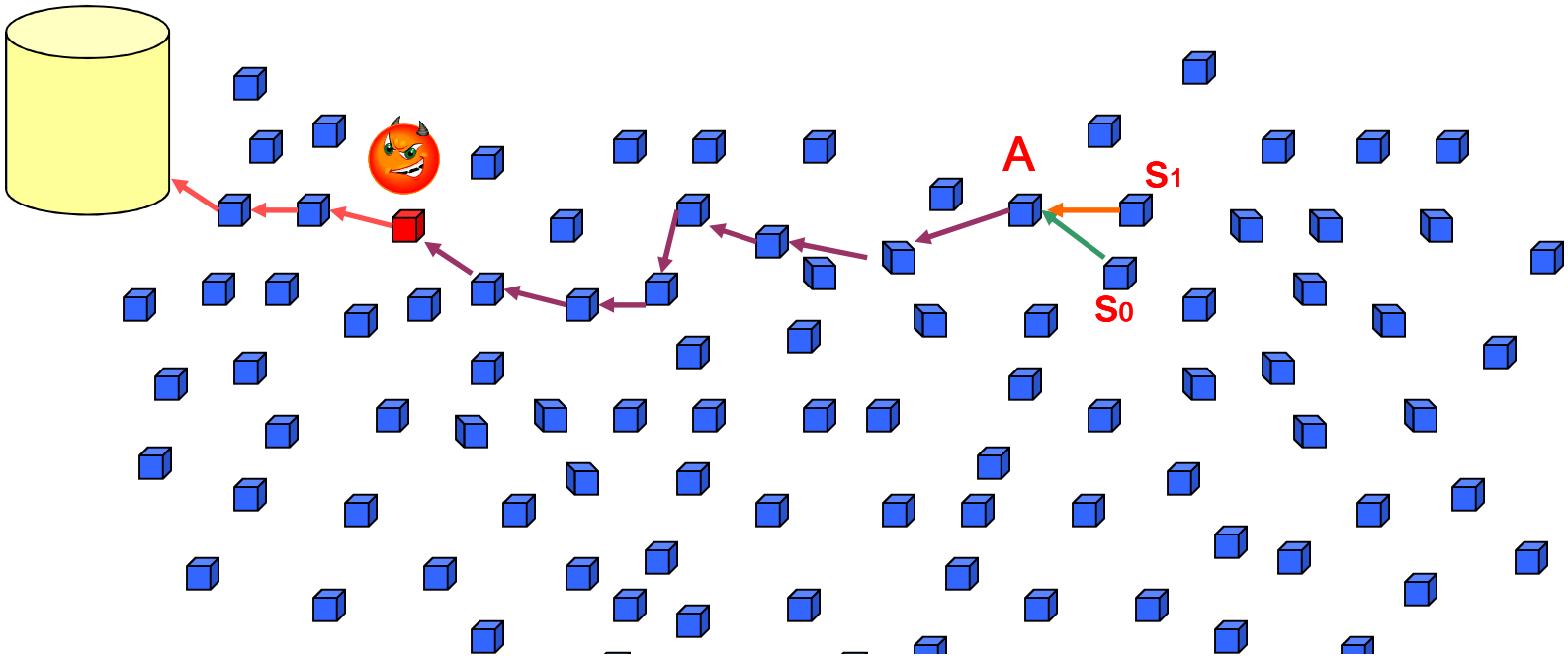
Sensor Data Aggregation



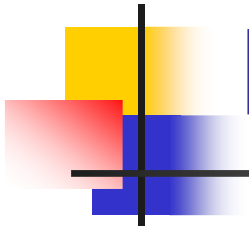
Aggregating messages in network saves resources.

Sensor Data Aggregation

Base station



This opens the risk that a single compromised wireless node can render the network useless or worse mislead the B.S into accepting a false readings.

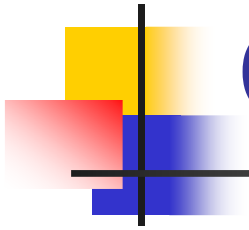


Data Aggregation Attacks

- Node Compromise: The attacker is able to reach any deployed sensor and extract the information stored on it.
- Sybil Attack: The attacker is able to present more than one identity within the network. The may create multiple identities to generate additional false data to alter aggregated results.

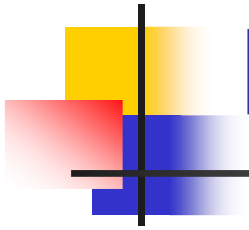
Data Aggregation Attacks

- Selective Forwarding Attack: The attacker refuses to forward the received message subsequently affecting the aggregation result.
- Replay Attack: The attacker records traffic from the network without even understanding its content and replays them later on to mislead the aggregator.



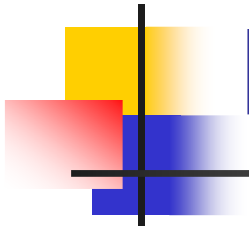
Contributions

- Survey of Secure Data Aggregation in Sensor Networks
- Propose adversarial model for secure data aggregation in sensor networks
- Framework for classification and comparison of sensor data aggregation



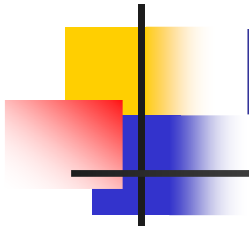
Existing Schemes

- Hu and Evans (2003) – Secure Data Aggregation (SDA)
- Jadia and Mathuria (2004) – Encrypted Secure Aggregation (ESA)
- Przydatek et al. (2003) – Secure Information Aggregation (SIA) uses aggregate-commit-prove framework
- Du et al. (2003) – Witness based data aggregation (WDA)



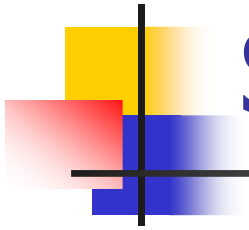
Existing Schemes

- Mahimkar and Rappaport (2004) – uses digital signatures (SecureDAV)
- Yang et. al. (2006) – Secure Hop-by-hop Data Aggregation Protocol (SDAP)
- Chan et. al. (2006) – Secure Hashed Data Aggregation improves on SIA (SHDA)



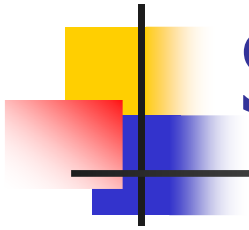
Existing Schemes

- Sanli et al. (2004) – Secure Reference Based Data Aggregation (SRDA)
- Westhoff et. al. (2006) – Concealed Data Aggregation (CDA)
- Castelluccia et al. (2005) – based on homomorphic encryption (EDA)



Security Requirements

- **Data Confidentiality**: ensures that information content is never revealed to anyone who is not authorized to receive it.
  - Hop-by-hop basis.
  - End-to-end basis.
- **Data Integrity**: ensures that the content of a message has not been altered during transmission process.
- **Authentication**: allows the receiver to verify if the message is sent by the claimed sender.



Security Requirements

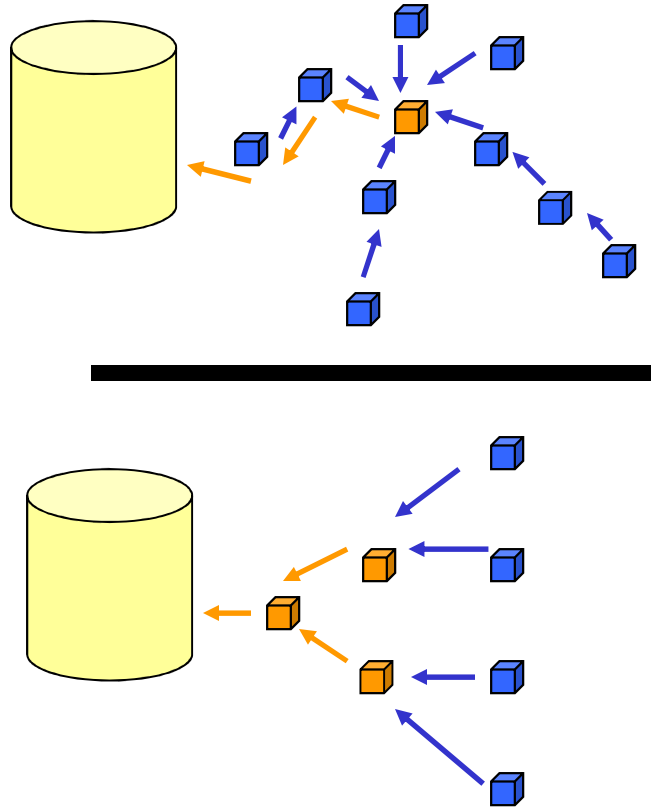
- **Data Freshness**: ensures that the data is recent and that no old messages have been replayed.
- **Data Availability**: ensures that the network is alive and that data are accessible. The data aggregation security requirements should be implemented to avoid extra energy consumption. If no more energy is left, the data will no longer be available.
- **Data Accuracy**: One major outcome of any aggregation scheme is to provide an aggregated data as accurately as possible.

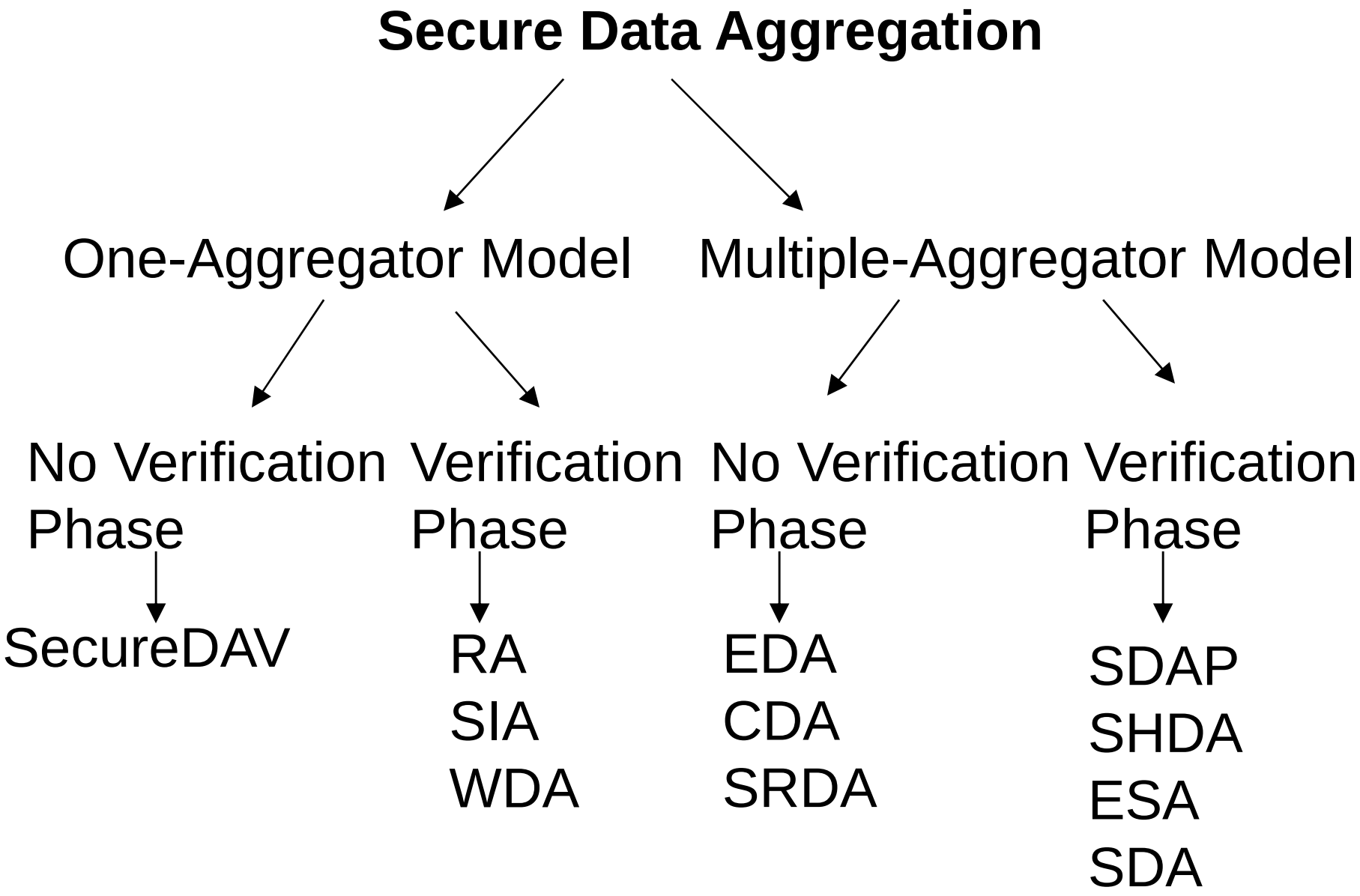
Security Services in Existing Schemes

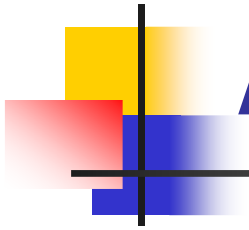
Scheme	Confidentiality	Integrity	Freshness
CDA	√		
SDA		√	√
SIA	√	√	√
SHDA		√	√
WDA		√	
SecureDAV	√	√	
SDAP	√	√	√
ESA	√	√	√
EDA	√		

Classification of Existing Schemes

- One-Aggregator model.
  - Verification phase or not.
- Multiple-Aggregator model.
  - Verification phase or not

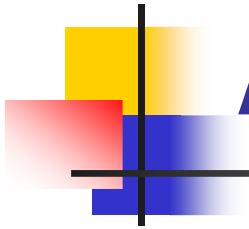



Secure Data Aggregation
One-Aggregator Model
Multiple-Aggregator Model
No Verification Phase
Verification Phase
No Verification Phase
Verification Phase
SecureDAV
RA
SIA
WDA
EDA
CDA
SRDA
SDAP
SHDA
ESA
SDA



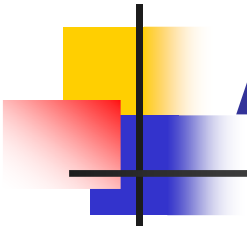
Adversary Model

- Adversary Type
  - Passive - This adversary eavesdrops on sensor communications
  - Active - This adversary interacts with the network injecting data, destroying nodes and destroying messages



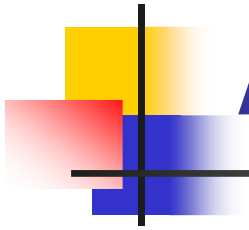
Adversary Model

- Network Access
  - Total Access - The adversary has total access to data transmissions
  - Partial Access - Adversaries can only observe or alter communications for a subset of nodes or messages on the network



Adversary Model

- Access to Secret Data
  - Total Access - The adversary has total access to secret data stored on the node. The node is fully compromised. The adversary often has high computational strength
  - Partial Access - The adversary has access to some of the data stored on the node.



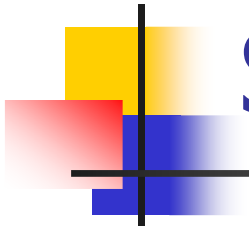
Adversary Classes

- Strong Adversary
  - Active Adversary, Total Network Access, Total Data Access
- Medium Adversary
  - Active adversary, low computational strength but may have partial access to data, Partial Network Access
- Light (Weak) Adversary
  - Passive Adversary, Limited Network Access

Attacks Defended Against in Existing Schemes

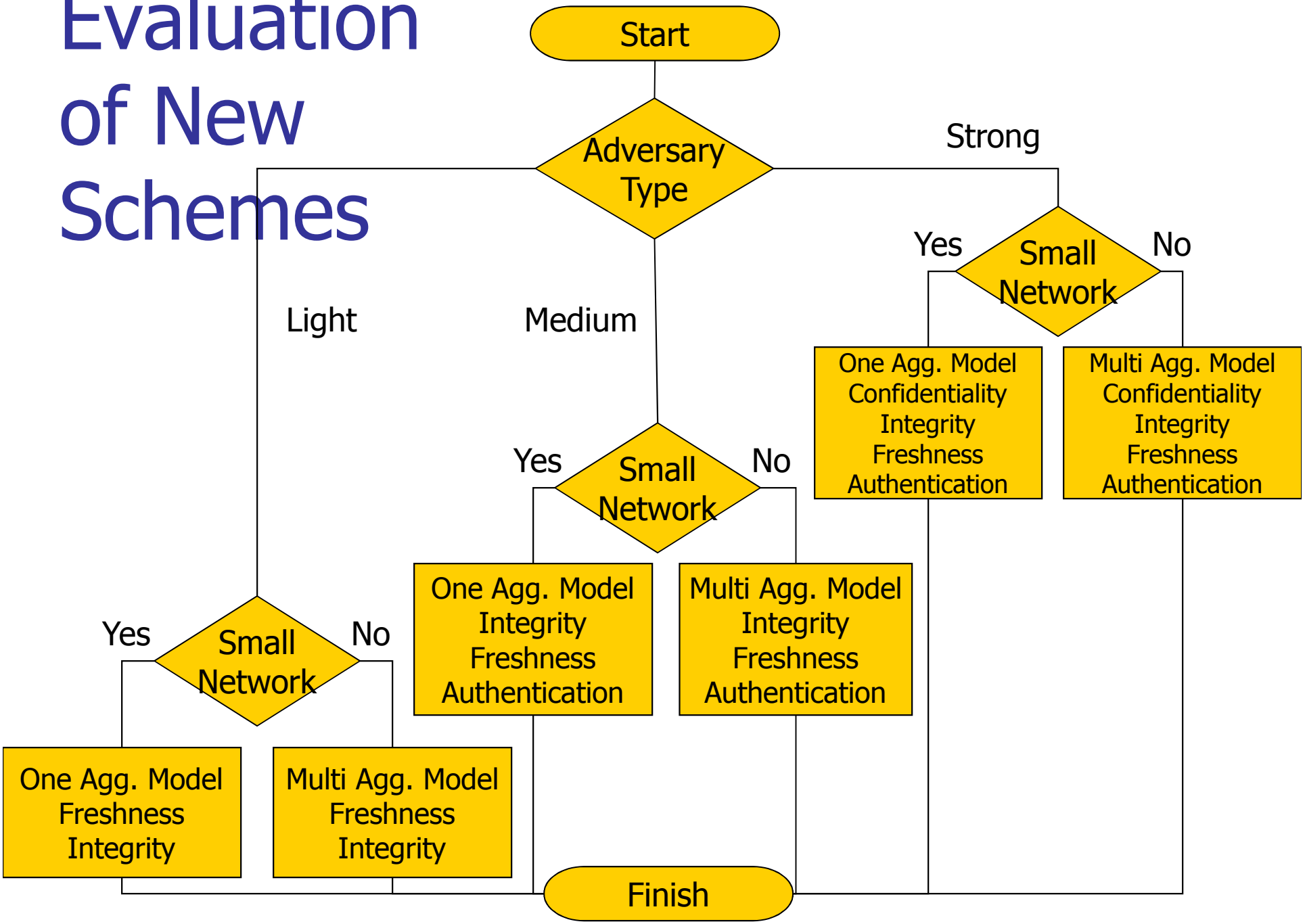
Scheme	Node Compromise	Replay	Selective Forwarding	Sybil Attack	Adversary
CDA					Light
SDA	√		√		Med
SIA	√		√		High
SHDA	√		√		High
WDA	√	√	√	√	Medium
SecureDAV	√	√	√		Medium
SRDA					Light
SDAP	√		√		Medium
ESA	√		√		Medium
EDA					Light

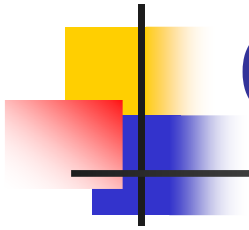
Adversaries in Existing Schemes



- CDA, EDA and SRDA meet minimum security requirements for a Light Adversary
- SDA, ESA and SDAP meet minimum requirements for a Medium Adversary
- WDA and SecureDAV do not offer data freshness
- SIA and SHDA meet minimum requirements for a Strong Adversary

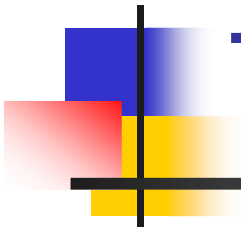
Evaluation of New Schemes





Conclusion

- Identified common adversary model and security requirements for secure data aggregation
- Future work
  - Formalize adversary model and develop tools/simulators for the model
  - Use adversary model to evaluate schemes
  - Extension of classification framework



Thank you

Questions?