A Security Infrastructure for Massive Mobile Data Distribution

Jesseildo Gonçalves
FranciscoJoséSilva
Department of Computer Science
Federal University of Maranhão (UFMA)
Brazil
jesseildo@gmail.com
fssilva@deinf.ufma.br

Rafael Oliveira Vasconcelos
Gustavo Luiz Baptista
Markus Endler
Department of Informatics
Pontifical Catholic University of Rio de Janeiro
Brazil
{rvasconcelos, gbaptista, endler}@inf.puc-rio.br
Motivation

- The recent transition from traditional networked computing to mobile networks, where mobility is a key aspect

- Support to tens or hundreds of thousands of mobile-networked nodes in an efficient and affordable way is a challenge

- Information security is a first-class necessity for many networked-systems and services, such as mobile-networked systems
Motivation

Applications such as fleet management, workforce coordination, Intelligent Transportation Systems, rescue and emergency management, environmental surveillance, etc.

- Have massive communications and traffic sensitive data

- The potential impact of disclosing this data can be problematic in many aspects, ranging from simple economic loss to increase of risk to life
Scenarios

Potential problems of plain transmission of position data and messages to/from mobile nodes:

**Example 1:** Intelligent Transportation Service tracks position and speed of metropolitan buses (of private companies) to ensure that the vehicle’s trips happen according to schedule
- Some company could manipulate the position traces of its own busses or the other company’s vehicles
- To obtain economic advantage, such as to catch more passengers for the own vehicles

**Example 2:** Remote monitoring and coordination of a police task force assault (for capturing criminals) by a Control and Command Center (CCC)
- Criminals could escape or better defend against police if they were able to intercept or manipulate, the police agent’s position data or the commands from the CCC
Goals

Design and validate an approach for secure mobile data distribution, that:

- Supports confidentiality, integrity and authenticity among both stationary and mobile nodes
- Introduces low-overhead on the system
- Is able to scale up to thousands of mobile nodes without compromising the communication performance
- Is modular and built upon a middleware for mobile data distribution
ContextNet and SDDL

- A middleware architecture for real-time sharing and processing of mobile context information, enabling real-time monitoring, communication and coordination of the mobile nodes in large-scale mobile applications.

- The Scalable Data Distribution Layer (SDDL) is responsible for the reliable, efficient and secure communication among any nodes in the ContextNet system.
Scalable Data Distribution Layer (SDDL)

- Connects fixed nodes (Core Nodes) running in a DDS Domain and deployed in a cloud to Mobile Nodes (MNs) that have an IP-based data connection

Supports 3 communication modes:
- Unicast
- Groupcast
- Broadcast

...between any fixed and any Mobile nodes and among Mobile nodes

Each application message can have any set of tags attached to it. They inform which type of data is being transmitted
Data Distribution Service™ (DDS)

- OMG® standard for real-time Pub/Sub that aims to provide efficient and low-latency data distribution middleware for large-scale systems
- Completely decentralized P2P architecture
- Data-centric model, where communication data structures are defined by topics and their properties
- Supports a large array of QoS policies (Durability, Reliability, Latency Budget, etc.)

Main APIs of SDDL

- **ClientLib - API for mobile client nodes**
  - Hides all MR-UDP protocol details and handles several connectivity issues with the Gateways on the SDDL core network
    - Handovers
    - Reconnections
  - Asynchronous communication thought listeners
  - Uses MR-UDP protocol
    - Light-weight protocol with temporary disconnection management

- **Universal DDS Interface (UDI) - API for SDDL Core nodes**
  - Simplifies the set-up and configuration of DDS entities
  - Abstracts from the idiosyncrasies of each DDS product
  - DDS Topic-independent

The Security solution should be build upon these APIs, and implement end-to-end security between the peers interacting through each topic.
SDDL Security Infrastructure - Requirements

- The security layer should add a minimum overhead in message processing and managing connections;

- Should be orthogonal to the use of multicast communication (in DDS domain);

- Data encryption should be independent of the SDDL communication mode (uni-, group- or broadcast), and the communication direction;

- The security protocols should have low resource consumption, specially in the mobile devices.
Each application defined topic is associated with a symmetric key used for encrypting and decrypting the data published on it.
SDDL Security Infrastructure - Architecture

- **Gateway**: responsible for intermediating the communication between mobile nodes and the SDDL network core

- **Key Distribution Center (KDC)**: responsible for perform the Key management and node authentication
  - The distributed Symmetric Keys have a validity and have to be periodically requested by the Publishers and Subscribers

- **Certificate Authority (CA)**: responsible for the generation, validation, and maintenance of digital certificates
  - Asymmetric cryptography is used for the authentication process
  - Digital certificates are generated by the OpenSSL tool and are included in each (Fixed or Mobile) Node that is part of the application
MNSL and FNSL responsibilities:

- Initiating the authentication and key distribution protocol,
- Managing a local database with the cryptographic keys for all topics used by the application
- Encrypting and decrypting (using symmetric encryption) data published and received through these topics
SDDL Security Infrastructure - Protocol

CtID: client ID
CERTct: client certificate
K_ac(T): certification ticket
Kct+: encryption using client public key
K: topic symmetric key
Client publishes a *SessionKeyRequest* message

At first, client does not have a certificate ticket
KDC publishes a ValidateCertificate message

If the message contains the certificate ticket, KDC itself tries to validate the ticket if not expired
CA tries to validate the certificate and publishes an instance of
ValidateCertificateResponse or InvalidCertificate
KDC publishes AuthenticationSuccess or AuthenticationFailed.

The symmetric key replacement process for each MN is on demand, i.e., only when there is a request for publishing or reading a topic instance. Along with the symmetric key, the MNs gets also remaining duration time of the key.
Experimental Setup

A Desktop executing: one Gateway, KDC, CA and simple test server application (using wired connection)

Two notebooks, executing NodeSimulator, a program which emulates any number of MNs (using wireless connection)

Each simulated MN periodically (each 30 seconds) sends encrypted coordinates, and receives an encrypted reply from the test server application
Evaluation Results:
Round Trip Delay Overhead

- **Round Trip Delay (RTD):** from the sending of each application message until the reception of the corresponding reply, by each simulated MN

- **Overhead introduced:** 50-75%
Evaluation Results: Communication Throughput

- How many pairs of send & reply messages the system is able to handle in a 30 minute time-frame
- Overhead introduced: insignificant
Related Work

Some DDS vendors have their own security solution:

- **PrismTech's Secure Networking Service (SNS)**
  - Based on symmetric keys and configurable cipher algorithms and key sizes
  - High configurability, integration with OpenSplice DDS's Network scheduler
  - Apparently, not supported for Mobile Nodes (i.e. OpenSplice Mobile)
  - Does not support session keys with limited validity (i.e. this may compromise the overall security)

- **RTI Secure WAN Transport**
  - Based on SSL/TLS and RSA encryption with public key infrastructure
  - Provides certificate-based authentication and confidentiality
  - Focus on WAN transport instead of mobile communication (no support for RTI Connext Micro)

- **Our previous work** (Gonçalves and Silva, 2013) extends DDS Topics to the mobile nodes, instead of using ClientLib
  - Facilitates development for mobile devices
  - Increases Gateway complexity and overhead, since it requires a large amount of Topic-specific Data Readers and Data Writers
Conclusions

- The presented solution supports confidentiality, integrity, and authenticity among both stationary and mobile nodes.
- It also realizes secure communication that scales to thousands of mobile nodes.
- The hybrid use of symmetric and asymmetric encryption has low computational cost.
  - Introduces minimal overhead in data processing and communication.
- End-to-end security increases security and does not add any overhead to the Gateway.
- Though KDC and CA are centralized, neither of them adds overhead to the encryption of the messages.
  - Additional KDC instances may be added at runtime.
Conclusions

- The security associations among the nodes are defined by simple tags on the messages (for each Topic)

- This solution can be extended to ensure the secure communication of the Data-Centric Publish/subscribe communication model promoted by DDS

- The evaluation has yielded encouraging performance results (low impact on performance)

- As future work, we intend to provide a context-aware access control mechanism for defined topics with spatial-temporal access restrictions
  - E.g. users would only be allowed to publish/subscribe to a specific topic when they are in a given location for the next two months
Thank you!

Q&A

For more information:
www.lac.inf.puc-rio.br
endler@inf.puc-rio.br
fssilva@deinf.ufma.br