



IoT Security – Autumn 2024

Practice Exercises for Lab Test

Manh Bui
School of Electrical and Data Engineering
Email: DucManh.Bui@uts.edu.au

Contact

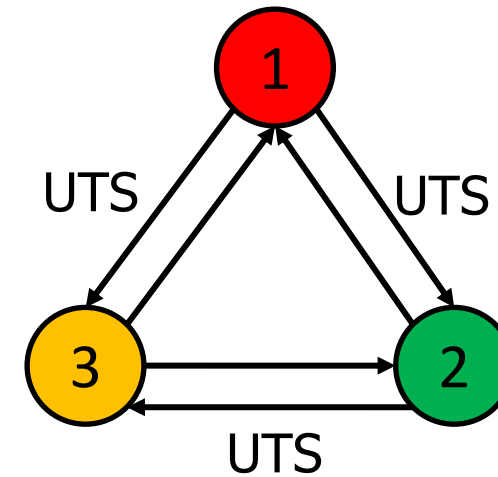


- Name: Manh Bui
- Email/Teams: DucManh.Bui@uts.edu.au

Exercise 1



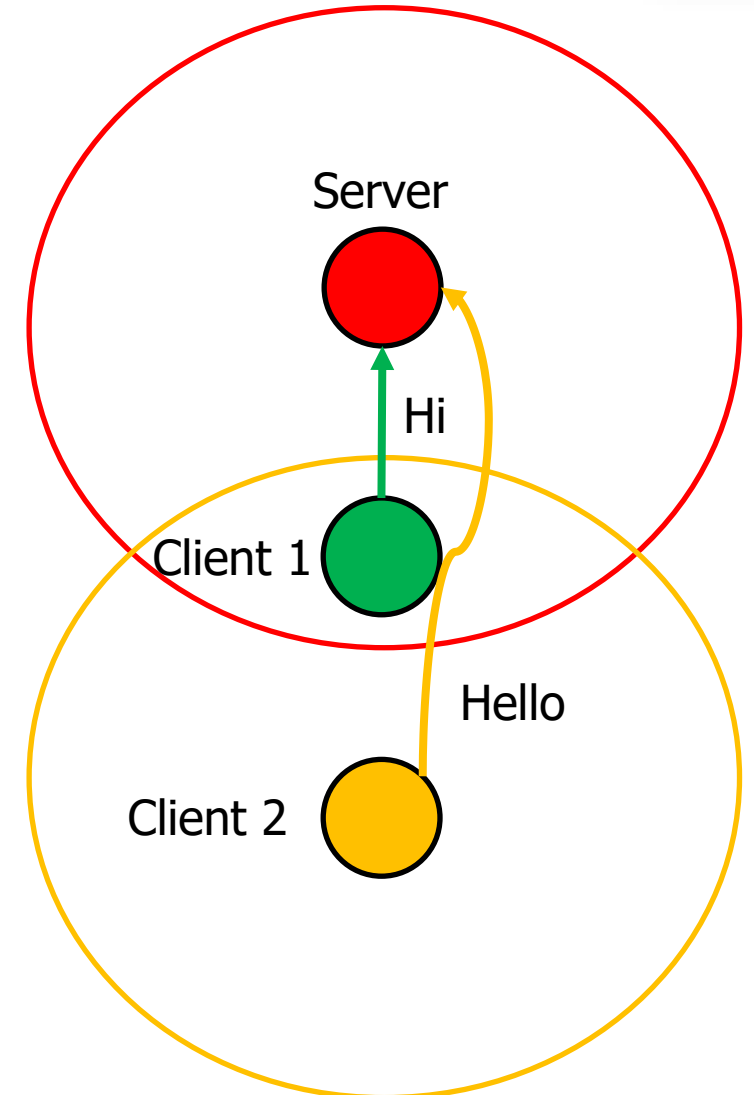
- Establish an IoT network with 3 sky motes to demonstrate broadcast communication using Cooja simulator.
- Make the motes to broadcast "UTS" message to other motes in the network. Capture the traffic of the network using Wireshark.
- Code for the motes:
`/contiki/examples/rime/example-broadcast.c`



Exercise 2



- Establish an IoT network with one UDP server and two UDP clients using Cooja simulator.
- Client 1 is in the transmission range of the server.
Client 2 is in the transmission range of Client 1 but not in the transmission range of the server.
- Make Client 1 send a message "Hi" and Client 2 send a message "Hello" to the server
- Modify the codes for UDP server and client
`contiki/examples/ipv6/rpl-udp/udp-server.c`
`contiki/examples/ipv6/rpl-udp/udp-client.c`

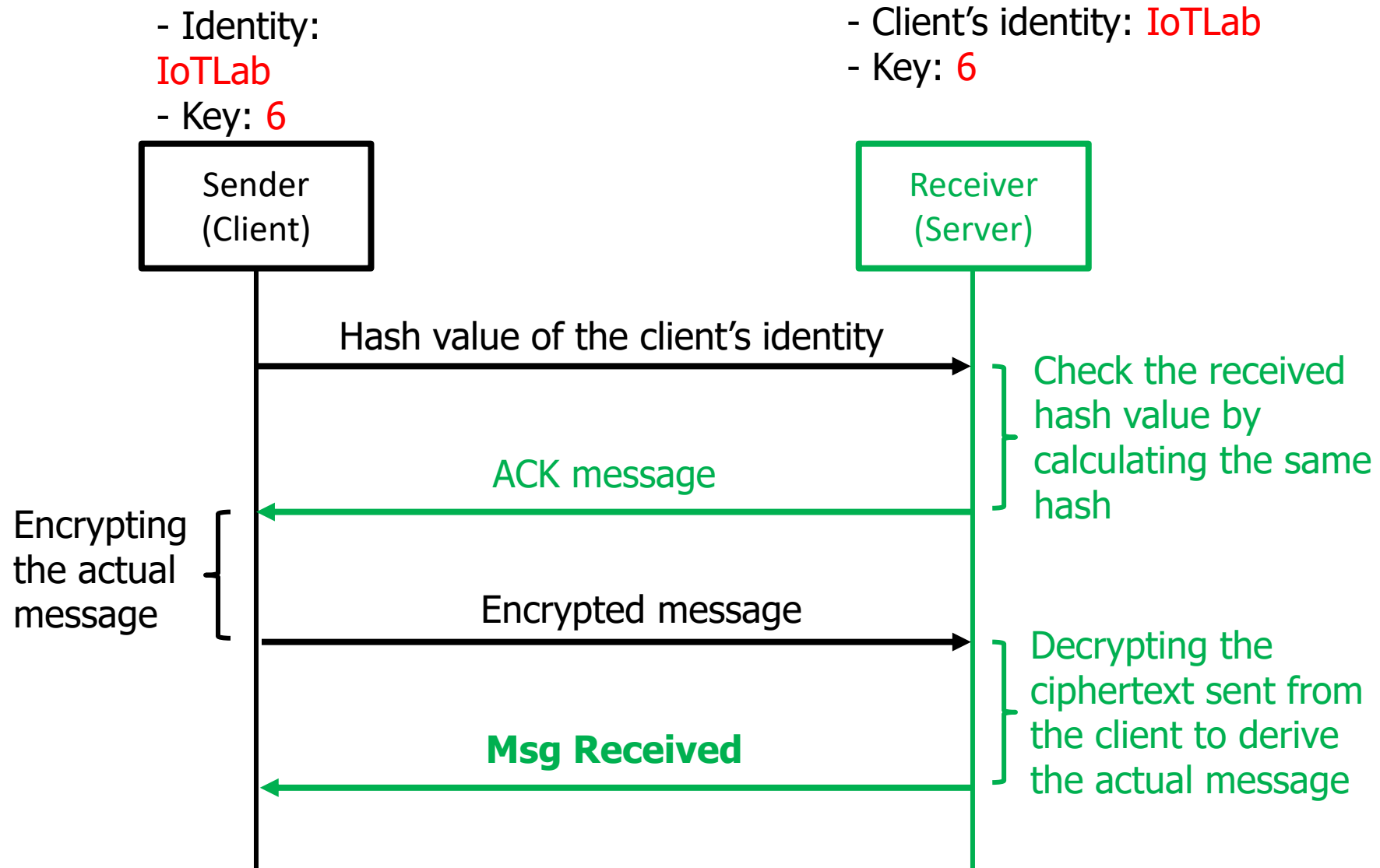


Exercise 3



- Establish an IoT network with one UDP server and one UDP clients to demonstrate IoT-Security/Authentication on RPL-UDP communication using Cooja Simulator.
- Construct the network by placing the client within the range of the server.
- Client's identity "**IoTLab**" is registered with the server. The client uses SHA-256 hashing algorithm to calculate the hash value of its identity and send to the server.
- Print the changed Client's identity to the mote output
- Upon receiving the hash value from the client, the server checks the received hash value by calculating the same hash.
- After successfully validate the client's identity, the server sends an **ACK** message to the client.
- Upon receiving the **ACK** message, the client encrypts its message "**Secret**" with Caesar cipher and sends to the server.
- The server decrypts the message with the same encryption algorithm and send message "**Msg Received**" to the client.
- Both the client and server are using the same key value (**key = 6**) for encryption and decryption.
- Codes: **receiver_authentication.c** and **sender_authentication.c**

Exercise 3



Exercise 4



- Establish an IoT network with one RPL border-router and 4 CoAP servers.
- Construct the network by placing CoAP server 1, 2, and 3 in the range of RPL border-router, CoAP server 4 is out of the range of the RPL border-router.
- Use Firefox to see the information of network, i.e., network topology.
- Use Firefox to remotely control the LED on the sky motes.
- Capture the traffic of the network using Wireshark tool.

References



1. Get Started with Contiki: <http://www.contiki-os.org/start.html>
2. Contiki Tutorial:
[http://anrg.usc.edu/contiki/index.php/Contiki tutorials](http://anrg.usc.edu/contiki/index.php/Contiki_tutorials)
3. [https://anrg.usc.edu/contiki/index.php/RPL Border Router](https://anrg.usc.edu/contiki/index.php/RPL_Border_Router)
4. [https://github.com/contiki-ng/contiki-ng/wiki/Documentation:-
CoAP](https://github.com/contiki-ng/contiki-ng/wiki/Documentation:-CoAP)
5. A. L. Colina, A. Vives, A. Bagula, M. Zennaro, and E. Pietrosemoli, "IoT in 5 days" [Online]. Available:
<http://www.iet.unipi.it/c.vallati/files/IoTinfivedays-v1.1.pdf>

