Supporting Secure Communication in Distributed Environments

Roman Špánek
Technical University of Liberec, Hálkova 6, 461 17, Czech Republic
Academy of Sciences of the Czech Republic, Pod Vodárenskou s veží 2, Praha 8, Czech Republic
Pavel Pirkl
Technical University of Liberec, Hálkova 6, 461 17, Czech Republic

Motivation

- Interaction between entities with very limited knowledge about themselves can take place only if trust between the parties is high enough.
- trust is not a static phenomena;
- new relationships may emerge,
- existing relationship may disappear or
- level of trust may change during the time.

- A motivation scenario: *Assume user A being asked for personal information by user B. User A can reject the request, or accept it. However, if user A cannot find out to whom the data will be sent, it should better reject the request. This, however, will lead to the situation when all requests are rejected. On the contrary, if user A is able to find out who user B is, he will make the decision whether share information or not much more easily.*

Virtual Organization Model

- Virtual Organization structure is represented as an oriented hypergraph
- where : $H = (U, N, W_U, W_N)$
- users equal to vertices U
- hyperedege N represents a group of users
- W_N stands for the security level of a group
- W_U represents user‘s abilities

Implementation

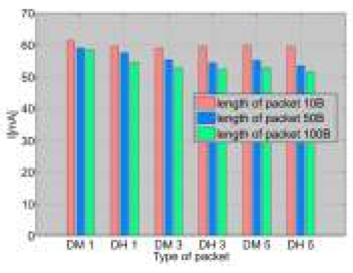
- the platform should be well accessible
- the platform should be widely known to as many users as possible
- the platform should be supported across environments
- the platform should offer unbound wireless communication support

=> *mobile phones*

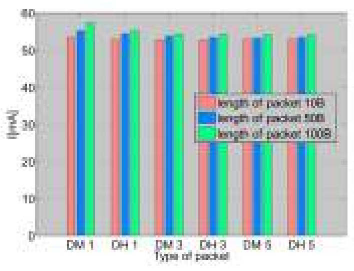
MyKeys

- Experimental implementation MyKeys,
  - programmed in J2ME
  - JSR-82 for Bluetooth support
- MyKeys offers a storage and management for user keys
- MyKeys supports concurrent connection up to 8 devices
- MyKeys supports Bluetooth service search
- MyKeys consists of few main classes, particularly:
  - Graphic User Interface
  - Bluetooth Server class
  - Bluetooth Client class
  - Data coding and encoding class
  - Record Management System (RMS) class

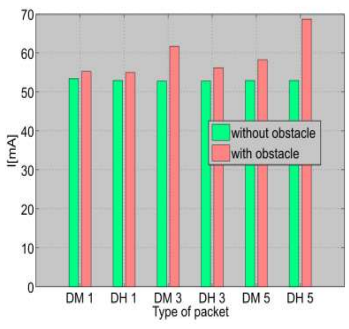
On Energy Consumption



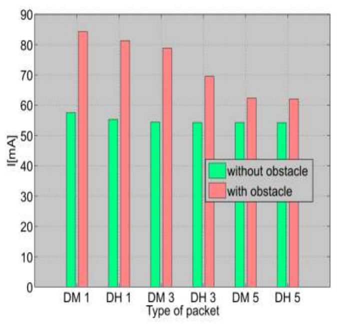
Measurement of energy consumption for continuous transmission



Measurement of energy consumption (repeated transmission with 100 ms period)

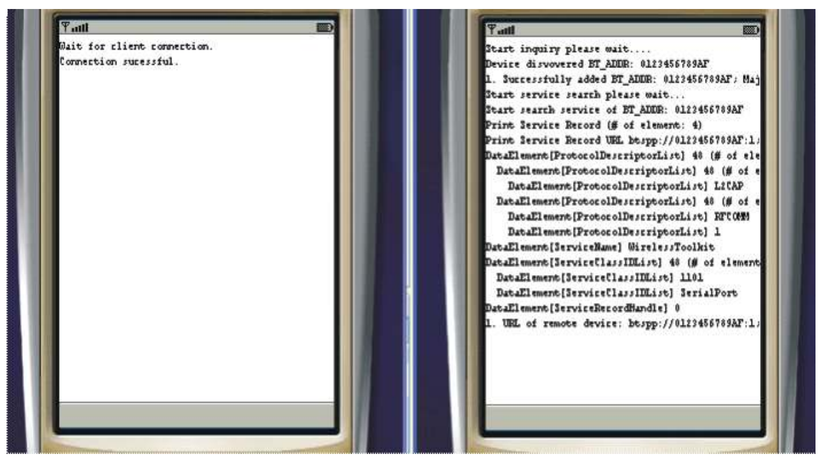


Measurements for 10 byte data with and without obstacle



Measurements for 100 byte data with and without obstacle

MyKey Implementation



```
Wait for client connection.
Connection sucessful.
```

```
Start inquiry please wait....
Device disvovered BT_ADDR: 0123456789AF
1. Successfully added BT_ADDR: 0123456789AF; Maj
Start service search please wait...
Start search service of BT_ADDR: 0123456789AF
Print Service Record (# of element: 4)
Print Service Record URL btspp://0123456789AF:1;
DataElement[ProtocolDescriptorList] 48 (# of ele
  DataElement[ProtocolDescriptorList] 48 (# of e
    DataElement[ProtocolDescriptorList] L2CAP
  DataElement[ProtocolDescriptorList] 48 (# of e
    DataElement[ProtocolDescriptorList] RFCOMM
    DataElement[ProtocolDescriptorList] 1
DataElement[ServiceName] WirelessToolkit
DataElement[ServiceClassIDList] 48 (# of element
  DataElement[ServiceClassIDList] 1101
  DataElement[ServiceClassIDList] SerialPort
DataElement[ServiceRecordHandle] 0
1. URL of remote device: btspp://0123456789AF:1;
```

- MyKey application was tested on Nokia 6600 and N70 mobile phones
- MyKeys verified connectivity of current mobile phones
- In a clear area mobile phones were discovered up to 33 meters
- Services were discovered up to 30 meters.
- Indoor abilities are highly limited by the surroundings
- Generally indoor distances were round 10 meters

Conclusion

- A novel approach for treating trust in a distributed environment is described
- The approach utilizes ideas from reputation systems based on social network
- Structure of Virtual Organization is modeled by a hypergraphs supporting dynamics of the VO
- MyKey experimental application for mobile phones provides keys exchange and management in a real environment on real devices
- Currently available Bluetooth devices are experimentally compared on energy consumption, accessibility and connectivity

Acknowledgement

- The work was supported by the project 1ET100300419 of the Program Information Society (of the Thematic Program II of the National Research Program of the Czech Republic) ``Intelligent Models, Algorithms, Methods and Tools for the Semantic Web Realization'', partly by the Institutional Research Plan AV0Z10300504 ``Computer Science for the Information Society: Models, Algorithms, Applications'' and by Ministry of Education, Youth and Sports of the Czech Republic, project No. 1M4674788502 – Advanced Remedial Technology and Processes.