A Security Scheme for Home Networked Appliances

School of Computing and Mathematical Sciences Liverpool John Moores University

Mazhar Ul Hassan,

Dr. David Llewellyn-Jones, Prof. Madjid Merabti

JMU

Liverpool John Moores University

OUTLINE

- P2P Networking
- Applications
- Challenges
- Networked Appliances
- Background Research
- Proposed Design
- Implementation
- Conclusion and Future Work
- Questions

P2P NETWORKING

- Peer-To-Peer Networks (P2P)
  - The term peer-to-peer refers to the concept that in a network of equals (peers) using appropriate information and communication systems, two or more individuals are able to impulsively work together without necessarily needing central coordination
  - Decentralized in nature
  - In P2P model, each node takes the role of both client and server
  - The decentralized nature of P2P networks facilitates scalability
  - In a P2P network, peers can join or leave the system without any intervention from a centralized server, which facilitates seamless integration of any number of new nodes (peers) to existing systems
  - The distributed nature of the P2P network adds robustness in the network as data is often replicated on different peers

APPLICATIONS

- P2P networks are used in situation where an infrastructure is not available or to deploy one is not possible

- P2P networks could be used in some business environment where the need of communication might be more important in meetings out side the office

- It can also be used to provide network services in disaster recovery
  - An infrastructure could be setup quickly in places affected by natural disaster

- P2P network could turn dream of highly adaptive technology needed to manage multi-hope network clusters

CHALLENGES

- There are many known challenges in the area of P2P network. Some of these challenges are security, dynamic network topology, routing and power efficiency.
- One of the concern is to provide secure communication in P2P network which is otherwise difficult due to its unique characteristic.
  - If no security mechanism is adopted then attacker can easily exploit P2P network
- Due to dynamic nature of P2P network it could suffer with frequent topology changes. The node can establish routing as they move about.
- A routing mechanism is required to establish an effective transmission in P2P network
- In P2P network routes are formed via combination of mobile nodes. This could force mobile node to be in awake mode most of the time. This could consume battery power and could disturb the overall network operation

NETWORKED APPLIANCES

- “A dedicated function consumer device with an embedded processor and a network connection”

- A device that publishes their functionality as services which can be discovered and used by other Networked Appliances, which extend the functionality beyond what they otherwise provide

- In future many houses will have networks, so that not only conventional data appliances (such as computer, phone, TV, wi-fi, camera and mp3 player) will be connected all or much of the time, but other appliances too (lights, central heating, fridge, washing machine and so on),

BACKGROUND RESEARCH

A number of research initiatives such as UPnP, HAVi, OSGi and NASUF have tried to standardize how devices are interconnected

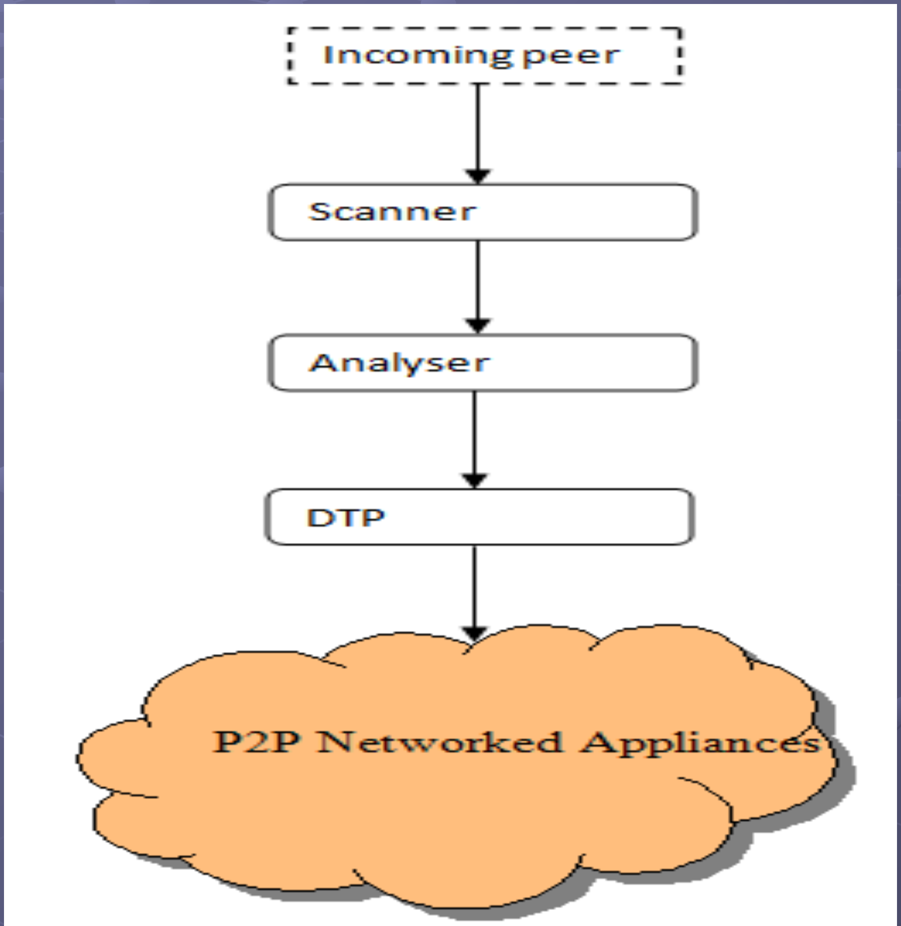
- UPnP (Universal Plug & Play)
  - + Automatically detected by the OS
  - + For LAN not for WAN
  - - No concept of services but set of Protocols
  - - No security
- OSGi (Open Services Gateway Initiative)
  - + Service oriented architecture
  - + Deploys services over WAN's to LAN's and devices
  - + Consists of a gateway between Internet and home network
  - - Centralized approach therefore whole network will fail in case of failure of central service
  - - Service usage is manually performed
  - - OSGi specification adopts ACL which is not suitable for P2P networking due to its lack of flexibility
  - - Lack of security

- ePerSpace
  - + Global Network Integration and Interoperability which allows interconnecting audio and video to exchange its content between distributed services in a secure manner.
  - - Difficult to implement in pervasive ad-hoc environments as it is a choreographed solution
  - - Users need authentication , not fit for P2P
  - - No security
- NASUF (Networked Appliance Service Utilization Framework)
  - + Self-oriented architecture. It provides mechanisms that allow networked appliances to be seamlessly interconnected and offer the services they provide.
  - + Concept of services
  - + Appliances offer/advertise their services to other appliances when needed
  - + Services discovered dynamically & composed within P2P network without any centralization
  - - Lack of security

- *It is known that due to number of reasons, these standards do not full-fill the criteria of a secure solution. That makes security an important challenge.*

PROP OSED DESIGN

HOME NETWORKED APPLIANCES SECURITY SCHEME (HNASS)



Interaction between HNASS security services

➢ Home Networked Appliances Security Scheme (HNASS)

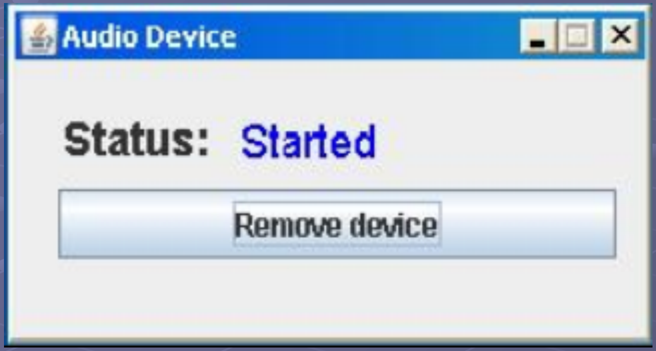
The Home Networked Appliances Security Scheme (HNASS) takes an intermediate approach between the existing schemes and some of the new concepts which have been developed.

- In HNASS all peers go through a combination of security checks before being able to utilize available services. Scanner, analyzer and a Decision Taking Peer (DTP) work together to provide the necessary security.
- In HNASS a scanner scans all incoming peers and views their unique IDs (UIDs), which are provided by JXTA.
  - The JXTA protocols enable device to discover and communicate
  - In addition it also support mechanisms for interoperability in between devices
- In addition, HNASS collects relevant security properties of the peer
- As well as details of connections with other services, forwarding the results on to the analyzer.
- The analyzer needs these three types of information from the scanner, and uses them to decide whether to allow or deny the incoming peer access.

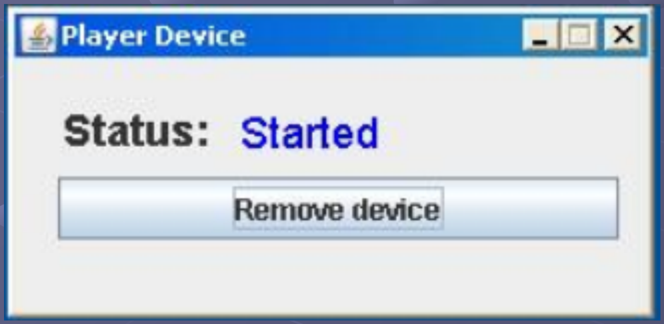
HNASS (1)

- In fact, the analyzer cannot take a direct action, other than making decisions about incoming peers.
- The result is therefore sent to the DTP (Decision Taking Peer) which will either allow or deny a peer based on the analyzer's decision.
- HNASS has been designed to provide an effective security solution for peer to peer network in Home Appliances
- It address the problem in a unique manner while taking into account some interrelated issue.
- HNASS could also be extended to support similar operation in the related network.

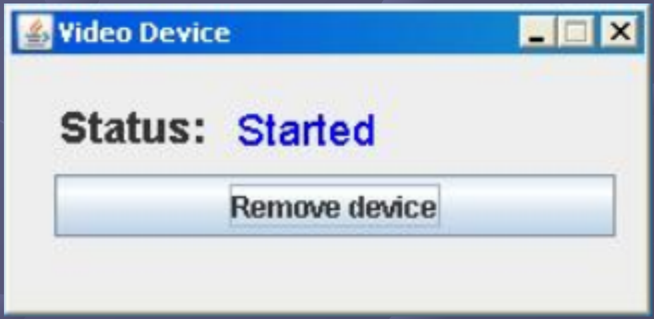
IMPLEMENTATION



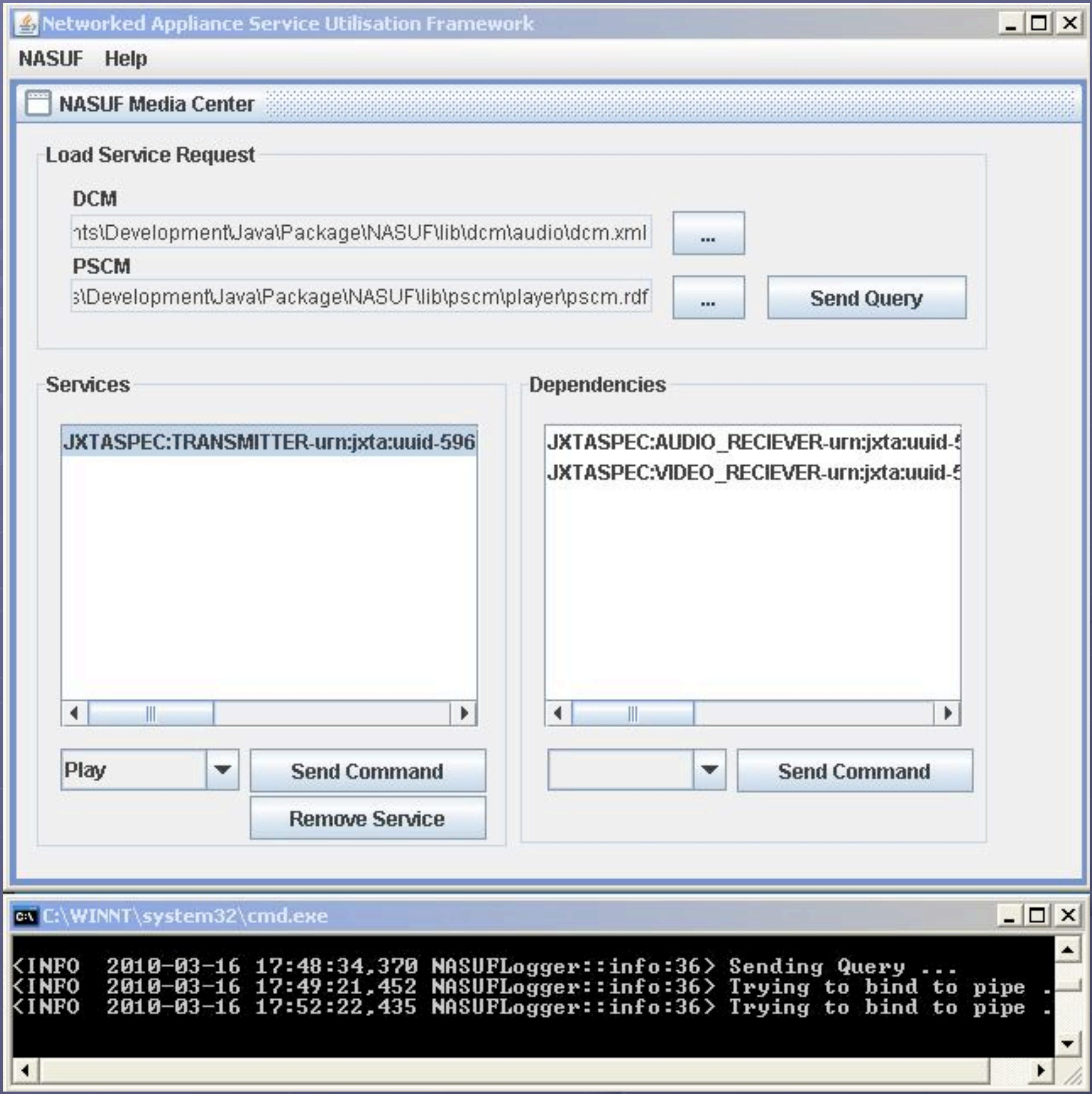
Status: Started



Status: Started



Status: Started



DCM: ıts\Development\Java\Package\NASUF\lib\dcm\audio\dcm.xml

PSCM: s\Development\Java\Package\NASUF\lib\pscm\player\pscm.rdf

Services:

JXTASPEC:TRANSMITTER-urn:jxta:uuid-596

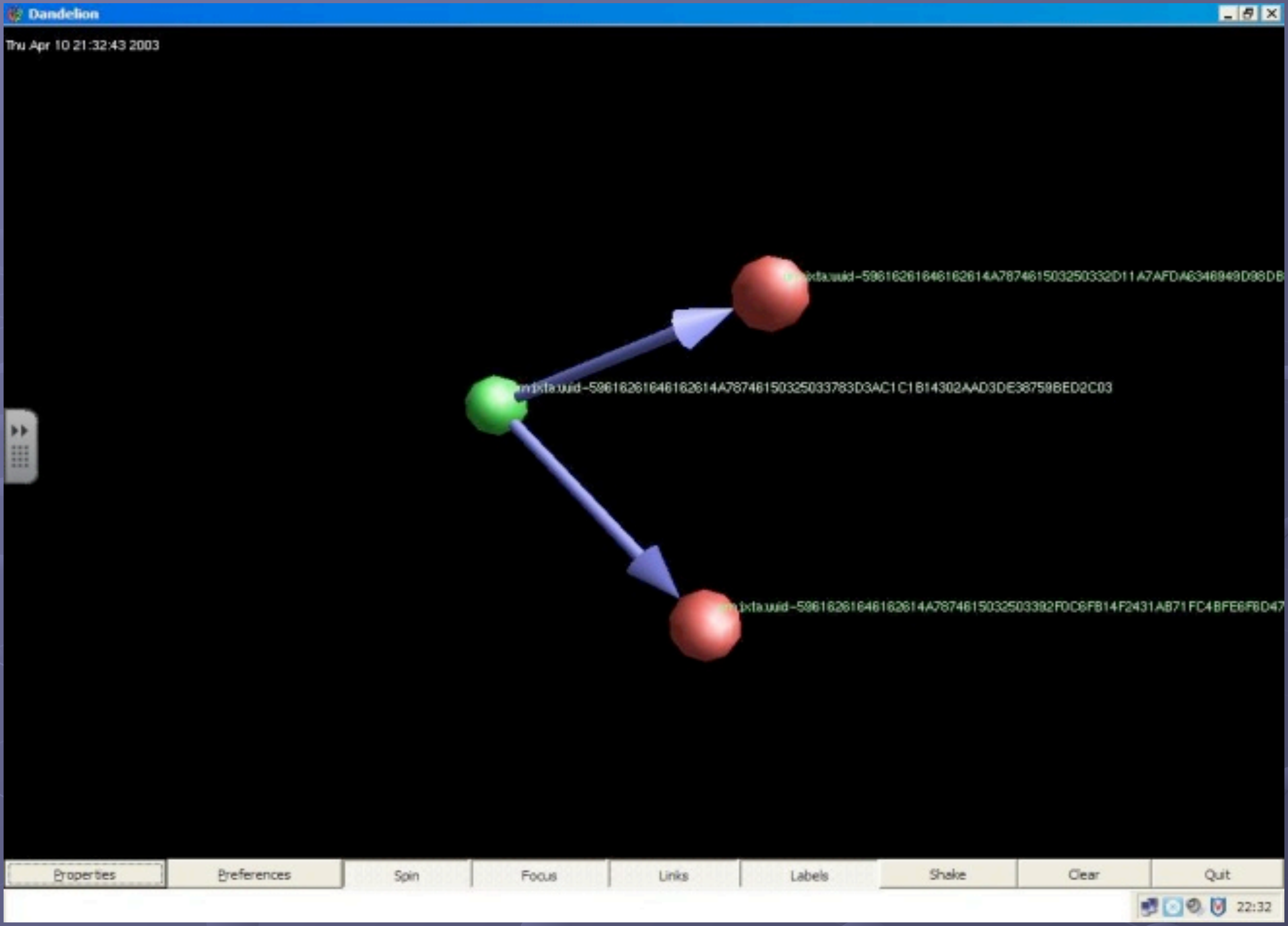
Dependencies:

JXTASPEC:AUDIO_RECIEVER-urn:jxta:uuid-5

JXTASPEC:VIDEO_RECIEVER-urn:jxta:uuid-5

Play

```
<INFO  2010-03-16 17:48:34,370 NASUFLogger::info:36> Sending Query ...
<INFO  2010-03-16 17:49:21,452 NASUFLogger::info:36> Trying to bind to pipe .
<INFO  2010-03-16 17:52:22,435 NASUFLogger::info:36> Trying to bind to pipe .
```


Dandelion
Thu Apr 10 21:32:43 2003
urn:jxta:uuid-59616261646162614A7874615032503332D11A7AFDA6346949D96DB
urn:jxta:uuid-59616261646162614A787461503250333783D3AC1C1B14302AAD3DE38759BED2C03
urn:jxta:uuid-59616261646162614A78746150325033392F0C6FB14F2431AB71FC4BFE6F6D47
Properties
Preferences
Spin
Focus
Links
Labels
Shake
Clear
Quit
22:32

Visual view of Peers after scanning process

CONCLUSION AND FUTURE WORK

- We have proposed a novel security mechanisms for peer to peer environment
- We believe that HNASS can provide a reliable solution to the peer to peer network
- HNASS not limited to NASUF can give impressive results in any other frame
- The scheme has been implemented and we are conducting further experiments to measure the performance of the developed
- HNASS utilizes a combination of three components to provide secure communication
- We have successfully scanned audio, video and player devices on the basis of their UIDs and properties
- We have not yet implemented Decision Taking Peer (DTP)

QUESTIONS

For question please drop me an email

mazhar77@gmail.com