

Network Discovery Mechanisms for Fast-handoff

Ashutosh Dutta, Sunil Madhani[#], Tao Zhang
Telcordia Technologies
Yoshihiro Ohba, Kenichi Taniuchi
Toshiba America Research Inc.
Henning Schulzrinne, Columbia University

Abstract: Proactive handoff mechanisms involving secure pre-authentication and proactive configuration help reduce the delay and transient data loss for real-time communication during movement between homogeneous or heterogeneous access networks. Pre-authentication is meant to perform authentication with a network before a mobile moves into the network. To achieve secure pre-authentication with a target neighboring network, a mobile needs to obtain an IP address of the authentication server from the target network when the mobile is still outside the target network and then to establish a security association with the authentication agent in the target network. This requires the mobile to discover the parameters of various network elements in the target network ahead of time so that the mobile can communicate with these network elements to establish proactive security associations. We describe several approaches for a mobile to discover the network elements in target networks before moving into these target networks. We also describe how network discovery can help provide fast-handoff using secure pre-authentication and proactive IP address acquisition during handover between different access networks.

1 Introduction:

As the evolution of wireless networking based on wireless LAN (Local Area Network) and cellular technologies progresses, and as mobility services prevail and people become increasingly mobile, it is more important for a mobile device to be able to find an appropriate point of network attachment that meets the application requirements and the characteristics of the mobile, in a timely, accurate and efficient manner. We refer to such functionality as network discovery. The functionality to discover network information can be used to better support mobility and mobile services. For example, to reduce interruptions to on-going application sessions during a handoff, a mobile device could perform pre-authentication with a target network before it starts the handoff into the target network. To do so, the mobile will need information about the neighboring networks, such as the address of the authentication server in the target network, before the mobile moves into the target network. We will refer to the process in which a mobile discovers information about its neighboring networks as network neighborhood discovery.

An important problem in network discovery process is the discovery database construction problem: how to construct a

database of network information in an automated, dynamic and efficient way? Solving this problem is not trivial in a multi-provider environment where a network provider may not be willing to disclose any network information of its own network to other network providers that compete with it, while it may provide detailed network information of its own network to its subscribers for better services. However, there has been no practical solution to solve this problem.

Rest of the paper is organized as follows. Section 2 describes the related work in the area of network discovery. Section 3 describes the proposed AIS discovery scheme and associated architecture. We present the database schema in Section 4. Section 5 describes the testbed architecture in details. We provide an experimental example of proactive handoff using network discovery scheme in Section 6. We finally conclude the paper in Section 7.

2 Related Work

There are many protocols and related work designed for service discovery and network discovery. However, none of these protocols provides support for

- Discovering information about neighboring networks at a higher layer
- Dynamic construction of the discovery databases
- Determining what information to collect and provide to mobiles.

Instead, the existing service discovery mechanisms focus on how to retrieve information already existing in databases. They rely on all local network providers to implement service information servers, which is too strict to be deployed in public networks.

Several service discovery protocols and architectures exist today including SLP [1], JINI [2], UPnP [3], Salutation [4], and LDAP [5]. However, they focus mostly on how a user retrieves service-related information assuming that the information is already available in the databases. The service-related information and hence the servers that hosts the information can be organized into a hierarchy, for example, in a way similar to the Internet Domain Name System (DNS). The service-related information can either be pre-configured or provisioned dynamically on the servers.

The information can then be updated either by human administrators or automatically by servers themselves exchanging updates with each other.

In cellular networks such as GSM and CDMA, the pilot signals of the mobile such as BCCH and Sync channels respectively, provide the details of the neighboring networks and report to the serving MSC (Mobile Switching Center). Serving MSCs use this information to decide who could be the target networks for the mobile.

Recently, some efforts have been underway to design discovery protocols that are specifically used to support network neighborhood discovery at several layers. A representative example is the Candidate Access Router Discovery (CARD) protocol [6] that provides network discovery mechanism at layer 3. A candidate access router is an access router in a neighboring network to which the mobile device may move into. CARD is designed to be used by a mobile device to discover a candidate access router, before the mobile performs IP-layer handoff into the neighboring network, in order to support seamless IP-layer handoff. With CARD, a mobile listens to layer-2 identifiers such as IEEE 802.11 BSSIDs broadcast from the radio Access Points (APs) in neighboring networks prior to making a decision about IP-layer handoff. The mobile then sends these layer-2 identifiers to the access router in its current network, which will in turn map the layer-2 identifiers with the IP addresses of the candidate access routers in the neighboring network and then send the candidate router addresses back to the mobile. Using CARD to support network neighborhood discovery leads to some limitations including the need to upgrade the routers in the network.

Similarly there are few task groups within IEEE 802.11 standards that propose few network discovery mechanisms at layer 2 and application layer. IEEE 802.11u [20] working group proposes methods of network selection with other external networks such as cellular. IEEE 802.11k [19] working group proposes 3 different ways of discovering networks around an access point. However this discovery mechanism is limited to 802.11 access only and takes advantage of layer 2. Recently IEEE 802.21 working group is considering using Information Service mechanism that provides information discovery at application layer. Some of the techniques introduced in this paper are being discussed currently in IEEE 802.21 WG.

Gloserv [7] is a service discovery architecture that provides several types of services that may include event, location-based services, communication and web services. Gloserv architecture is similar to DNS as it contains root name servers and authoritative name servers that manage the information services. It can have some high level categories for name servers such as events, services, people or places. Gloserv architecture provides sets of services such as registration ability to announce one's services, querying

ability with local user agents for a certain set of services from the server. Gloserv uses RDF schema to define the sets of services and it uses Sesame for creating and storing RDF records. Sesame can use HTTP, Java RMI or SOAP as part of its querying mechanism.

This paper describes a new architecture to support network discovery including methods to solve the discovery database construction problem and methods for mobiles to discover information regarding neighboring networks. The proposed architecture is referred to as Application-layer mechanisms for Information Service (AIS). AIS is designed to be extensible enough to support current and future types of network information that may be needed by mobiles. AIS leverages existing protocols as much as possible. Although information about the network elements can have multiple usages, we focus on discovering the information a mobile can use to enable proactive handoff and secured pre-authentication and discuss how these information can be used to support secured and proactive handoff.

Information construction process, information retrieval methodology, format of the information stored in the information server are some of the key design factors that need to be looked into while designing the discovery architecture.

3 AIS-based Service Discovery Architecture

We have designed several architectures for AIS (Application Information Service). They can broadly be classified into two main categories: *network-assisted* and *mobile-assisted*. In the following sections we describe these architectures and how different functional elements can interact with each other. In each of these architecture alternatives, the mobile will query an AIS server or a peer mobile to find out the information regarding the networking elements in the neighboring networks. The methods of constructing the information database differ in each different architecture. A network-assisted architecture can follow both the distributed and centralized model. The AIS server keeps the information about the network elements in the neighboring networks and will provide the information after getting a query from the mobile. In a centralized model, reporting agents in each network will report the information about the networking elements within the network by using SNMP MIB (Simple Network Management Protocol Management Information Base). The mobile-assisted model is always distributed in nature where the end nodes report the information about the networks they are visiting currently. The way in which the information is retrieved from the AIS server by the mobiles is common for both the approaches. Peer-to-peer based model is another mobile-assisted model where the mobiles act as the information server and provide the information to

other mobiles. We describe both database construction and information retrieval in the following paragraphs.

3.1.1 Discovery Database Construction

Information server-based architecture can be mobile assisted or network assisted. In the following sections we describe both end-node assisted and network assisted approaches for constructing a network information database.

3.1.1.1 Mobile-assisted approach

We propose a new paradigm for collecting, maintaining, and discovering local services and networking capabilities. The new paradigm will overcome the limitations of the existing approaches described in related work section. The proposed approach uses the following main principles:

- Each mobile user can use any proper means available to him/her to discover the network information available in a visited network. Often the user will not need any special assistance from the visited network solely for the purpose of discovering the information the subsequent mobiles may need regarding the visited network. For example, when a mobile connects to a visited network, it will learn the addresses of the access routers and authentication agents in the visited network as part of its normal process for connecting to the visited network. Such information can be reported to the mobile's AIS server which can in turn provide the information to subsequent mobiles before they move into this visited network so that the subsequent mobiles can retrieve the information. The discovery of an available hotspot network and its logon requirements also do not require the local network providers to provide any special assistance.
- Each mobile user reports the information it discovers in a visited network to its AIS server. A mobile's AIS server does not have to have any trust relationship with the network that the mobile is currently visiting.
- A mobile user's AIS server is responsible for maintaining the information regarding the network information received from its subscribers regarding different networks.
- When a subsequent mobile moves into a visited network, it may query its AIS server for local information it needs.

The proposed approach has the following main advantages over existing approaches:

- Information mining and discovery will not rely on the local network providers to provide information servers used to provide network information.
- Regardless where a mobile user is and which local network it currently uses, the mobile always uses a single protocol to communicate with its AIS server to retrieve network information.

- An AIS server only needs to maintain information its own subscribers are interested in. Furthermore, an AIS server only needs to maintain information regarding the locations its own subscribers travel to.

This allows the proposed paradigm to be highly scalable.

The basic operation of the proposed collaborative discovery paradigm is illustrated in Figure 1. It shows how mobile moves between the networks and can update the information about the network elements to a location server commonly shared by a set of networks. This information is stored in the location server using a specific format.

3.1.1.2 Network assisted information discovery

Network assisted information discovery defines three different primary methods:

1. Reporting Agent (RA) assisted,
2. AAA assisted
3. DNS-based approach

We briefly describe each of these mechanisms.

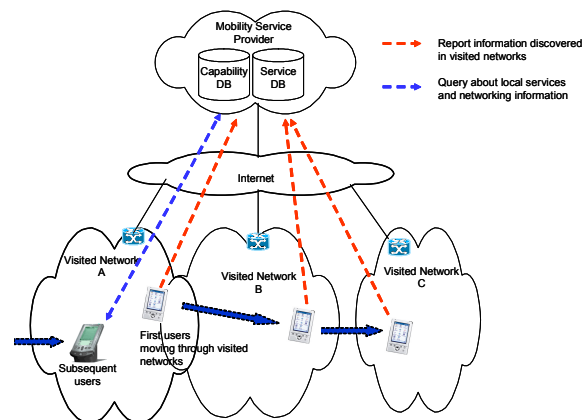


Figure 1: Discovery of local services and network capabilities.

3.1.1.2 Reporting Agent Assisted

Reporting Agents (RA) are network agents that reside within each network. These are SNMP capable and have the ability to collect the information about the network elements by probing the SNMP MIBs. These reporting agents (RA) will collect the information in the respective domains and populate the location server database for a specific region. This information may include capability set, IP address, geo-coordinates of the respective network elements in the network. When a specific network element is attached or becomes operational within a domain, its information is pushed onto the reporting agent (RA), which in turn is sent to the AIS server. Thus this approach provides a semi-

centralized way of populating the AIS server database compared to the end-system assisted approach described previously. The security concerns are less of an issue here as database update is provided by a specific networking agent instead of by the end client and there is a pre-established security association between the RA and the information server. Figure 5 shows an example of populating the database using information reported by the Reporting Agents.

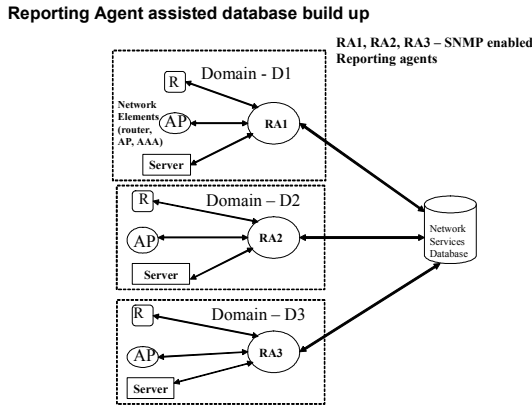


Figure 2. Populating the database using Reporting Agents

3.1.1.3 AAA Server Assisted

AAA (Authentication, Authorization, Accounting) [10] server assisted information building is another network server assisted approach. Information profile of the mobiles can be saved in the AAA servers as well. Any AAA protocol such as RADIUS and Diameter can be used for populating the network discovery database in a way that an AAA client sends a pair of an address of the mobile and an address of the AAA client to the AAA server. The pair is carried in Calling-Station-Id and Called-Station-Id attributes of the RADIUS and Diameter protocol. The AAA server can collect the information reported from the AAA client and keep track of the mobility pattern of the mobile by recording a list of tuples (the address of a AAA client, the time the mobile associated with the AAA client, the time the mobile disassociated with the AAA client) for the mobile. This list is then used for constructing the database of neighboring networks among which mobiles can perform handoff.

However this approach may not be applicable for multi-provider case where a service provider may not want to disclose its topological database to other competing service providers.

3.1.1.4 DNS Server-based approach

One can also use DNS SRV record to find out the list of these network elements instead of using the AIS server. DNS can always populate the services associated with the network elements (routers, APs) and their associated geo-coordinates using DNS's LOC record. Thus one can query a DNS server, give a list of services for a specific domain and

the range of geo-coordinates and get a list of network elements that provide these services. A general query may look like this. Given a specific geo-coordinate value, find a set of servers that provide a specific set of services such as routing, IEEE 802.11 and AAA. A combination of DNS "SRV" record and geo-location record (LOC entry) will help in determining a set of servers in the vicinity. Note that this approach is not intended for forming arbitrary structured network information database and may be limited by DNS's limited functionality of acting like a query server.

3.1.2 Database query process

Many of the operation such as authentication, IP address acquisition may be required during a mobile's movement between domains, subnets within a domain. These operations which are usually done after the mobile has moved to the subnet if done ahead of time help provide the fast-handoff. In order to perform these operation while in the previous domains or subnets it will need to communicate with the next hop routers and servers before the movement is over. Thus a mobile needs to discover the neighborhood information including the APs, routers, DHCP servers and several authentication agents such as PANA [9] (Protocol for carrying Authentication to Network Access) authentication agents and in some cases SIP (Session Initiation Protocol) [17] server before moving to the neighboring networks. Network discovery mechanism helps a mobile to perform several types of operation ahead of time such as pre-authentication and proactive IP address assignment.

We described several ways of populating this database in the previous subsection. The discovery process can also be centralized, distributed or peer-to-peer. As an example, a mobile can make a query to get the list of network elements providing routing service or authentication service in the subnet where a specific access point is connected. We provide an example of how the mobile can query the information service during the discovery process.

Initially a mobile boots up, obtains the IP address and configures itself with other network parameters such as default gateway, and several server parameters etc. It begins to communicate with a corresponding host and at certain point during its communication based on certain policy it determines that the mobile is impending to move. At that point the mobile initiates the AIS discovery process in one of several different ways. It can always use its location information as the look-up key while making a query. The location information can be the MAC address of the current access point, geographic address or any other civic address. When the MAC address of an access point is used as the look-up key, the mobile can obtain the MAC address either (i) by listening to beacon frames if the mobile is in the radio coverage of the access point or (ii) by recursively performing the query procedures where the recursion starts with specifying the MAC address of an access point known

to the mobile based on method (i). The server gets the query and reports back the list of attributes asked based on the query type.

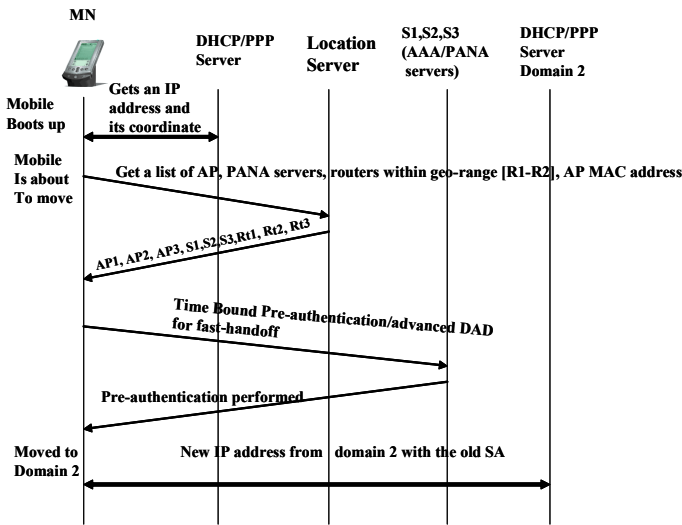


Figure 3: Protocol flow for network service discovery

If the client is GPS equipped it can always find its own location and determines where it plans to move and thus provides a range as part of the information look up and obtain the desired network information. Figure 3 shows a protocol exchange and sequence of operation for the network discovery. Figure 4 shows scenarios of a client discovering the neighborhood servers/routers ahead of time, so that it can get the addresses of the neighboring servers and routers where the mobile has the probability of moving. The range of geo-coordinates of the mobile and the MAC address of an access point are used as the look-up key for querying. Network discovery process helps discover the neighborhood servers, routers and access points ahead of time. By discovering the servers ahead of time pre-authentication can be performed thus expediting the handoff time during the movement. In figure 4, the mobile is currently attached to access point AP0 and has three neighboring networks D1, D2 and D3 where the mobile has the probability to move. Thus the mobile can query the AIS server with a specific key and can get the information regarding the neighboring APs, servers, and routers in domains D1, D2 and D3 with which it can communicate with to prepare for the secured handoff. We describe below a sequence of operation after a mobile is booted up.

1) A mobile boots up and connects to a specific Access Point. It obtains an IP address via an IP address configuration procedure such as DHCP or PPP. The When geo-coordinates are used as the look-up key, the range of geo-coordinates is associated with those IP address and delivered to the mobile together with the IP address during the IP address configuration procedure

as part of DHCP option. Thus the IP address of the AIS server for a specific region can be provided during the IP address configuration procedure or by DNS “SRV” record.

2) It may also happen that the neighboring cells may belong to different domains. From DHCP configuration, the mobile can find out its current domain (e.g., “att.com” or “sprint.com” etc.). It can also find out the domain names of the neighborhood areas using reverse DNS look up from the IP addresses of the network elements that were obtained.

3) The mobile makes a request to the AIS server using its currently attached AP and access router such as following

- 1) The request contains a list of network information types about which the mobile wants to retrieve (e.g., type=“PANA authentication server”, “router”) for a specific location (e.g., geo-location R0 or the MAC address of AP0), with specifying a condition (e.g., in the Geo-range [R1 --- R2] or “within 1 mile”). The condition could be determined based on the velocity of the mobile or mobility pattern.
- 2) The AIS server returns the list of network information (e.g., IP addresses of servers and routers, MAC addresses of APs that satisfies the condition specified in the request by querying its own database that has been populated separately.
- 3) From this information the mobile can have the list of probable networks that it is likely to move and

thus perform a time-bound pre-authentication and/or proactive IP address acquisition.

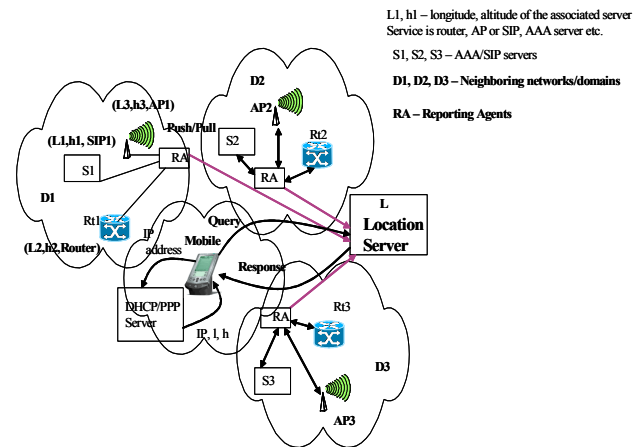


Figure 4. Geo-coordinate based network service discovery

There are additional features for database querying that AIS can provide. For example, the criteria used for choosing network information to be provided for a mobile can be either specified by the mobile or by the AIS server or by both entities. When the AIS server specifies the criteria, the profile of the mobile may be used as the criteria. In this case,

the AIS may provide detailed network information for mobiles subscribing to a high-class AIS service than mobiles subscribing to a low-class AIS service.

3.2 Peer-to-Peer Model

A peer-to-peer model does not depend upon the information server for information storage and retrieval. Instead, each mobile terminal will serve as an information server. We describe two peer-to-peer-based models, such as *scoped multicast* and *proactive broadcast*.

In the proposed peer-to-peer model,

- Each mobile moving between the networks keeps the information about the recently visited networks in its local cache for a specific duration
- Each neighbor of a mobile may have different information about the neighboring networks

3.2.1 Scoped multicast approach

- Each mobile announces their knowledge of visited networks on a localized multicast address M, with certain scoping and the amount of time they will like to keep it in the cache
- Based on the proximity of the network and probability of movement the mobile communicates with the designated peer to get the particulars of the network

Figure 5 shows an example of peer-to-peer based network discovery mechanism using scoped based multicast approach.

Figure 6 shows an example of peer-to-peer based network discovery mechanism using recursive broadcast approach.

There is no information server in this architecture and figure 7 shows how the mobile can discover about the other networks by querying the peers within the network.

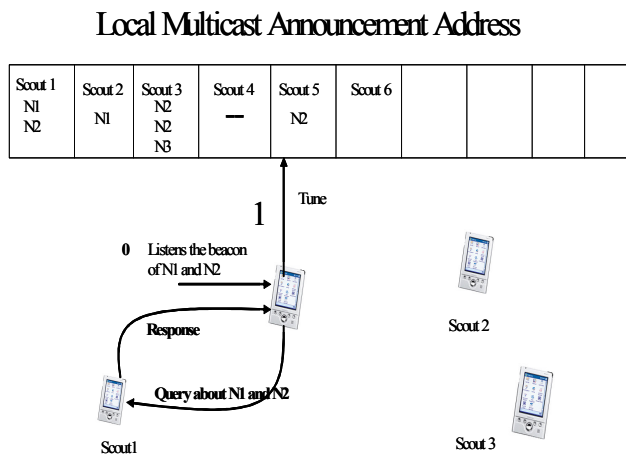


Figure 5 - Scoped-based multicast approach

3.2.2 Recursive broadcast approach

- Each mobile broadcasts recursively to find the information about a specific network within the network
- Broadcast can span beyond its own subnet

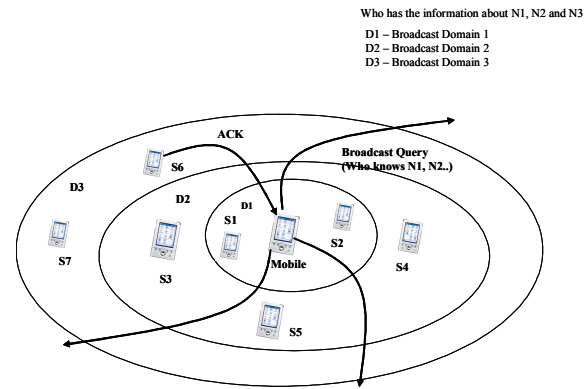


Figure 6 – Recursive broadcast-based approach

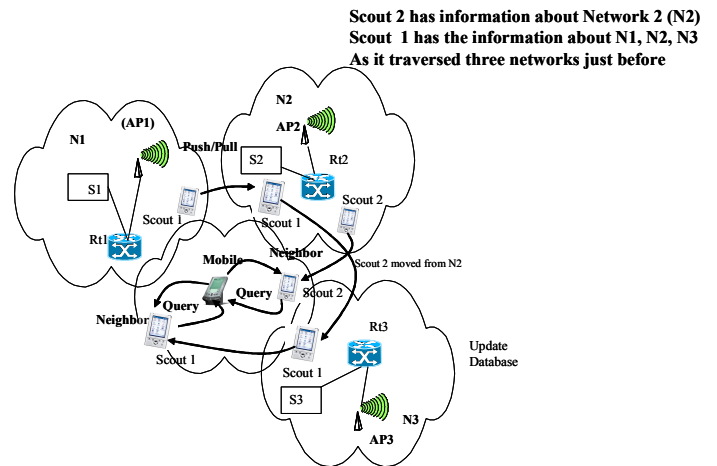


Figure 7. Peer-to-peer-based network discovery

This works under the assumption that the mobile carry a lot of information about the other networks and keep it in the cache for a specific period of time. The mobile can query this information proactively as it decides to move to other networks and obtains the information about the other networks. It also assumes that the mobile has the ability to communicate with its peers and extract this information. In some cases there may be a need to establish some security association between the mobile and its peers.

4 Database schema and implementation

This section describes a sample implementation of the query and response mechanisms needed to support network discovery. To query information related to a specific network interface (e.g., 802.11, CDMA), a mobile needs to first know which information attributes are supported by a network

interface. Thus a query-response mechanism may use two steps: the first query provides the meta-data information (i.e., the attributes' names) and the second query provides values of the attributes the mobile is interested.

Existing database querying mechanisms do not allow us to obtain detailed information of a specific network given a certain property such as network type, GPS coordinate of the mobile, etc. Such detailed information could be MAC address of the neighboring APs (Access Point), channel number associated with the AP, IP address of DHCP server, AAA server, and etc. Thus it is desirable to design a query mechanism that can support schema (or sub-schema) access. The query mechanism should also be extensible and should accommodate proprietary vendor definitions.

The information on the Information Server should be stored in a standard and easy to access manner. We have used RDF (Resource Description Framework) [8] based schema to describe and store the information regarding networking elements and their characteristics on the Information Server. RDF is a framework that describes a language for representing information about resources in the World Wide Web. It is intended for representing metadata, such as title, author, and modification date of a Web page, and copyright, about Web resources. RDF can also be used to represent information about other things that can be identified on the Web, even when they cannot be directly retrieved on the Web such as specifications, prices, and availability. RDF provides a common framework for expressing the information so that it can be exchanged between applications without loss of meaning. It is intended for describing information that needs to be processed by applications, rather than being only displayed to people. Therefore, RDF-based query and response mechanisms provide a suitable way for mobiles to report to and retrieve information from the application information server. It allows a mobile to query specific information elements about a network by providing the characteristics of the information elements in a granular manner. For example, network information elements in a network could be Access Points, DHCP servers, and authentication and authorization servers.

The characteristics of these network information elements could be SSID, location-info (geo-coordinate), layer-2 (L2) security information.

RDF schema defines the structure of the information elements as well as the relationship between the information elements. RDF schema is usually partitioned into two schema type; basic schema and extended schema. Basic schema is static and includes media independent classes and properties. Extended schema includes the properties that are dynamic in nature.

Figure 8 shows a very simple view of the RDF-based tree that we have used in our database construction. It shows the network elements in the neighborhood networks and the inter-dependency.

4.1 RDF schema design

We now illustrate sample RDF schema that can be used for information discovery. For the sake of brevity we have provided only a subset of the schema. We have selected to show examples that include combination of basic and extended sets of classes and their associated properties. For example a network class will have properties of type L2 and L3. An L2 class will have properties such as network-id, operator, location and neighbor information.

```
<?xml version="1.0"?>
<!DOCTYPE rdf:RDF [
  <ENTITY rdf 'http://www.w3.org/1999/02/22-rdf-syntax-ns#'>
  <ENTITY rdfs 'http://www.w3.org/2000/01/rdf-schema#'>
  <ENTITY mihbase 'URL_TO_BE_ASSIGNED'>
]>
```

```
<rdf:RDF xmlns:rdf="&rdf;" xmlns:rdfs="&rdfs;"
xmlns:mihbase="&mihbase;"
xml:base="&mihbase;">
```

```
<rdfs:Class rdf:ID="Network">
<rdfs:subClassOf rdf:resource="&rdfs;Resource"/>
<rdfs:comment>
```

Network class has two properties, namely I2 for layer-2 information and I3 for higher-layer information. Any property can be added to this class in an extended schema.

```
<rdfs:comment/>
</rdfs:Class>
<rdf:Property rdf:ID="I2">
<rdfs:domain rdf:resource="&#Network"/>
<rdfs:range rdf:resource="&#L2"/>
<rdfs:comment>
This property is of type L2 class.
<rdfs:comment/>
</rdf:Property>
```

```
<rdf:Property rdf:ID="I3">
<rdfs:domain rdf:resource="&#Network"/>
```

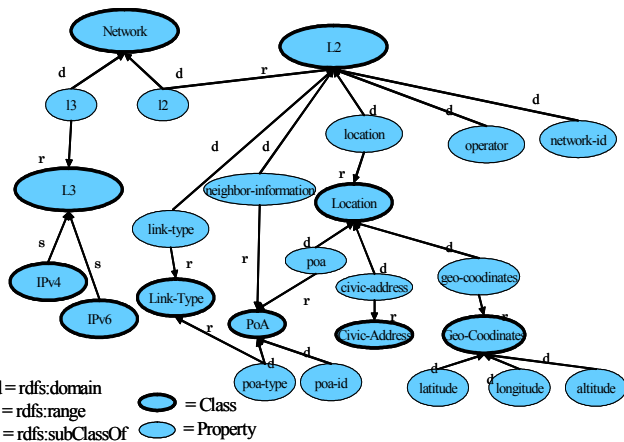


Figure 8: Schema inter-dependency diagram.

```

<rdfs:range rdf:resource="#L3"/>
<rdfs:comment>
This property is of type L3 class.
</rdfs:comment/>
</rdf:Property>

```

```

<rdfs:Class rdf:ID="L2">
<rdfs:subClassOf rdf:resource="#&rdfs;Resource"/>
<rdfs:comment>

```

L2 class has properties that are specific to link-layer. The properties include network-id, operator, location and neighbor-information properties. Any property can be added to this class in an extended schema.

```

<rdfs:comment/>
</rdfs:Class>
<rdf:Property rdf:ID="operator">
<rdfs:domain rdf:resource="#L2"/>
<rdfs:range rdf:resource="#&rdfs;Literal"/>
<rdfs:comment>

```

This property contains a name of the operator. It could be the same as network-id property.

```

<rdfs:comment/>
</rdf:Property>
<rdf:Property rdf:ID="network-id">
<rdfs:domain rdf:resource="#L2"/>
<rdfs:range rdf:resource="#&rdfs;Literal"/>
<rdfs:comment>

```

This property contains an identifier of the network. It may contain an SSID.

```

<rdfs:comment/>
</rdf:Property>
</rdf:RDF>

```

4.2 Schema primitives

We present sample primitives in ASN.1 format that can be transported as part of RDF schema.

```

Network ::= ENUMERATED {L2info, L3info, Location}
L2info ::= ENUMERATED {802.11, 802.16, GSM, GPRS, W-CDMA,
cdma2000}
L3info ::= ENUMERATED {IPv4, IPv6}
Location ::= SEQUENCE {
    Geo-location ::= String
    Civic-addr ::= String
}
802.11 ::= SEQUENCE {
    Standards ::= BITMAP {802.11a, 802.11b, 802.11g}
    SSID_Network_Name ::= String(SIZE(1..32))
    BSSID ::= NumericString(SIZE(6))
    Channel ::= INTEGER
    Phy ::= ENUMERATED {CCK, DSSS, OFDM}

```

```

Data_Rates ::= INTEGER
Network_Service_Provider_Code ::= String
Network_Service_Provider_Name ::= String
Network_Service_Provider_Tariff ::= String
Cipher_Suites ::= BITMAP {WEP, TKIP, AES-CCMP}
Authenticated_Key_Management_Suites ::= BITMAP {WEP, Psk, 802.1x}
KeyManagementProtocol ::= ENUMERATED {11i4WayHandshake}
Quality_of_Service ::= ENUMERATED {802.11e}
Cost ::= INTEGER
Roaming_List ::= String
Mobility ::= ENUMERATED {802.11r, 802.11u, 802.21,
PreAuth}
}
IPv4 ::= SEQUENCE {
    Router_Address ::= String
    DHCP_Server_Address ::= String
    DomainName ::= String
    Subnet ::= String
    SIP_Server_Address ::= String
KeyManagementProtocol ::= ENUMERATED {IKEv1, IKEv2}
Authentication ::= ENUMERATED {PANA, UAM}
PacketCipherring ::= ENUMERATED {IPsec}
Internet_Service_Provider_Code ::= String
Internet_Service_Provider_Name ::= String
Internet_Service_Provider_Tariff ::= ???
Mobility ::= ENUMERATED {MIPv4, CT, CARD,
PreAuth}
Quality_of_Service ::= ENUMERATED {...}
VPN_Gateway_Address ::= String
NAT_Address ::= String
}
MIPv4 ::= SEQUENCE {
    HomeAgent_Address ::= String
    ForeignAgent_Address ::= String }
PANA ::= SEQUENCE {
    PAA_Address ::= String
    EP_Address ::= String }

```

5 Testbed architecture and performance

This section provides an architecture and describes the functional components used in information query and update process. At the Information Server end, we use Joseki to interpret the RDQL [8] and send appropriate responses to the client. We use Jena [12] for forming RDQL. Jena is a Java framework for building Semantic Web applications. It provides a programmatic environment for RDF, RDFS and OWL, including a rule-based inference engine. The

implementation in Jena is coupled to relational database storage so that optimized query is performed over data held in a Jena relational persistence store.

We have used JOSEKI_server for publishing RDF models on the web. These models are represented by URLs and can be accessed by query using HTTP GET. Figure 9 shows the logical testbed architecture. Initially the mobile is in network 1, and is connected to access point AP1. Network 2, Network 3 and Network 4 are neighboring networks. The Information Server stores the information about these networks and the associated network elements such as authentication server, configuration server, Access Point ID etc. We have implemented both information updates and queries. First mobile updates the information. When a second mobile decides to move into one of these networks, it makes an RDF query and gets the meta information about the neighboring networks, and based on certain policy it queries the information server again to get other detailed information about the network elements within each of these networks. Table 1 shows the output of typical query and response. Table 2 shows the results that include both query 1 for meta data and query 2 for values of specific network elements. The mean and the standard deviation are reported in this table. Application layer delay includes upper layer interaction and is dependent upon the implementation type such as JAVA or C. Network layer delay includes delay due to TCP layer transaction.

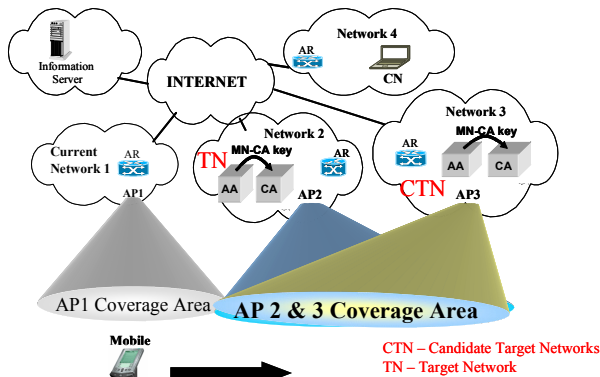


Figure 9: Logical architecture of the testbed

Processing delay includes processing time at the server for a specific query and transmission time for carrying the response from server to the client. In this experiment, during the transaction of query 1, mobile sends 1288 bytes of data and gets 1684 bytes as response. Query 2 involves 1713 bytes of data sent by the client and 1335 bytes of data sent by the server. Query and Responses are carried back and forth in chunks to accommodate the maximum segment size (MSS) thus adding to the delay little bit. Since these query and responses are carried as part of HTTP messages, TCP is the chosen transport method. Transport delays could be significantly reduced if UDP is used as a transport protocol instead. But then one needs to look into the reliability aspect of the transmission. We observed the average update delay by the client to be 353 ms with a standard deviation of 153. However this is not critical for handover decision. This

update time will of course depend upon the amount of data being updated and network bandwidth. Optimizing the query delay is important for the mobiles with high mobility rate as the mobile needs to make a decision based on the query. Processing power at the end clients and transport methods will help optimize the delay associated with the query and response. We found the delay due to query 2 to be less than query 1 because of additional ARP (Address Resolution Protocol) performed as part of query 1. Response to first query is the meta data, where the mobile finds out the relevant networks that are of type 802.11, and using tariff as the policy information it decides to get more information about other network elements such as access router, PANA server, and DHCP serve etc.

The IEEE 802.21 working group is currently considering using both XML and TLV format for information discovery. RDQL uses XML format for query and response. We did a preliminary performance comparison between XML and TLV format. The size of query and response obtained via RDQL are much larger than the size of TLV query and response. However if basic Schema is changed to more flat structure, then the size of query and response will be reduced. On the other hand XML-based query provides more extensibility and flexibility. Since the number of bytes going over the air is a concern, we have also tried to use compressed version of XML. By using the compressed version of XML during information query, it reduces the discovery time to some extent. We describe some examples of using integration of XML and TLV and some performance numbers of using the combination.

Table 1 – RDF Query/Response

Query	Response
Current PoA: AP1, Query list of 802.11 type neighboring networks with associated tariff values	Neighbor 0 PoA ID:00:20:A6:53:B2:5E Tariff: 20 Neighbor 1 PoA ID:01:23:45:67:89:AB Tariff:50
Neighbor 0 selected, Query a list of network elements for Neighbor 0	Target Network Channel: 10 SSID: ITSUMO newpoa1 Router address: 10.10.10.52 Router MACID: 00:00:39:e6:8b:ee Subnet: 255.255.255.0 DHCP Server

Table 2 – Query Processing Time

Delay components	Query 1 (ms)	Query 2 (ms)
Total Delay	2292	1473
Network Layer	919	451
Server processing	18	13
Client processing	64	48

In order to support the query and response in most cost effective manner it is important to provide extensibility, flexibility and efficiency. There are two possible candidate solutions, XML and TLV. XML provides schema-based semantic query but needs to send more bits over the air if one uses native XML 1.0 format. TLV provides binary encoding but does not provide a standard query language for semantic query. One possible approach to integrate these two is to convert XML data contained in the query result into TLV. XML data can be converted to TLV using two different methods. Method A is applicable to any XML data, and method B is applicable to a particular query language. XML-based query language has three types of query such as construction query, selection query and Boolean query. Construction query is used to fetch the sub-graph, selection query is used for selected bindings and Boolean query is used for “yes” or “no”. Table 3 shows some sample results showing how the query time is reduced by using a combination of XML and TLV or by using a compressed version of XML. Similarly selection query time and boolean query time also get reduced by using a combination of XML and TLV. On an average selection query results in a delay that is similar to construction query, but time for boolean query is much smaller than the other two queries because of the number of bytes. For example, boolean query byte size is one-tenth of selection query byte size and one-eighth of construction query byte size.

Table 3: Construction query using integrated approach

Construction Query		Method A	Method B	gunzip
Direct Conversion	Binary(TLV)to Internal	7 ms	9 ms	N/A
3Step Conversion	Binary to XML	14 ms	15 ms	15 ms
	XML to DOM	41 ms	41 ms	41 ms
	DOM to Internal	33 ms	33 ms	33 ms
	Total	88 ms	89 ms	89 ms

6. Network Discovery assisted Proactive handoff

This network discovery approach could be applicable to both heterogeneous and homogeneous handoff scenarios. The proposed network discovery mechanism can help several handover scenarios among heterogeneous systems including 802.11, 802.3, 802.16 and cellular networks.

Similarly movement among homogeneous Systems include

- Single interface e.g., 802.11, between ESS)
- Multi interface (e.g.,, 802.11, between ESS)

We then illustrate how network discovery process can be integrated to help provide secured and seamless proactive handoff.

As the mobile moves between the networks, the process of proactive handoff will primarily include two stages. First stage involves discovering the neighboring elements such as the next hop router, DHCP server, authentication agent and AAA server in the network the mobile is about to move and second stage involves setting up a secured pre-authentication based security association with the PANA authentication agent in the neighboring network.

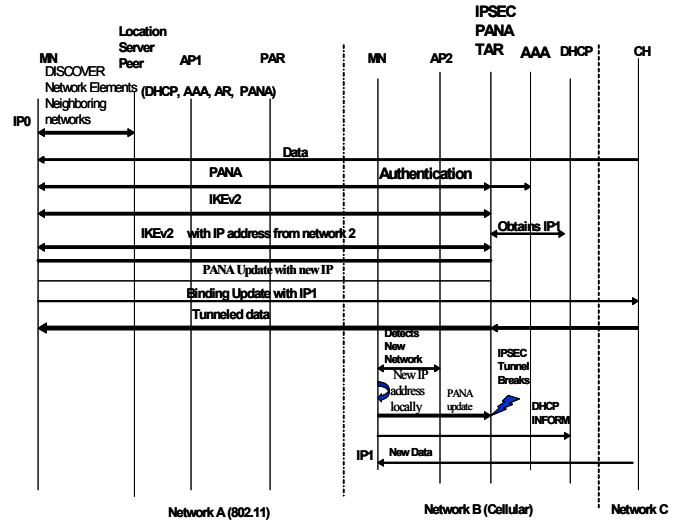


Figure 10. Protocol flow network discovery assisted handoff

During this secured pre-authentication the mobile can also obtain an address from the DHCP server in the next subnet. By having the pre-authentication process done ahead of time, the mobile will not need to spend time in setting up security association after moving to the new subnet. By having an IP address of the next subnet locally available, the mobile will also avoid the time spent for getting an address using DHCP process, although it may use DHCP INFORM to obtain all other configuration parameters. Figure 10 shows the protocol interaction between various elements during the transition between the access networks. Access networks A and B can be in two different administrative domains. Initially the mobile MN has an address IP0 assigned to it. As it is about to move, it performs the proposed network discovery process and obtains the MAC address of the neighboring networks. The mobile uses the MAC address of the access point as the identifier to query the network elements in the neighboring access networks using the schema described in section 4. These network elements include access routers, PANA authentication agents in the neighboring network. In order to perform a secured handoff the mobile sends a message to the PANA authentication agent that is usually co-located with the Target Access Router (TAR) in the neighboring access network. At this point IKE [11] (Internet Key Exchange) signaling sets up an IPsec tunnel between the TAR (Target Access Router) and the mobile. This tunnel is set up to make sure that the data is tunneled through and is secured. In the process of setting up the tunnel it also obtains an IP address from the DHCP

server that is resident in the target access network. The DHCP server will dispense an IP address (say IP1) from its IP address pool. The DHCP server may like to perform an ARP before handing out the IP address to the mobile through IKEv2. This IP address passed to the TAR through DHCP is then carried in a Configuration Payload of IKEv2 and finally is assigned to the mobile as the IPsec tunnel inner address. The mobile now has two IP addresses, i.e., IP0 and IP1. When the IPsec tunnel is implemented in the mobile as a logical tunnel interface (i.e., ipsec0) and the mobile has two addresses, i.e., IP0 for the physical interface (i.e., eth0) and IP1 for the virtual interface. At this time the mobile sends a binding update to the correspondent host (CH) or to the home agent depending upon the mobility protocol being used. After the binding update, CH or home agent sends the new data to the new IP address IP1. New data from the CH destined to IP1 will be captured by the TAR and will be tunneled via the established IPsec tunnel. Now as the mobile crosses over and connects to the new access point AP2, it gets an event trigger that will delete the old IPsec tunnel and will assign the new address IP1 to its physical interface (i.e., eth0). In cases where there is no IPsec tunnel established, a regular short-lived IP-IP tunnel is established between the mobile and the next router.

Since the mobile has obtained the IP address only that can be assigned locally, as the mobile moves to new network it may perform a DHCP INFORM so as to be able to configure other server parameters such as DNS server, DHCP server etc. As another option, these parameters can be obtained through the IKEv2 signaling during the establishment of IPsec tunnel between the mobile and TAR before the mobile moves to the target access network.

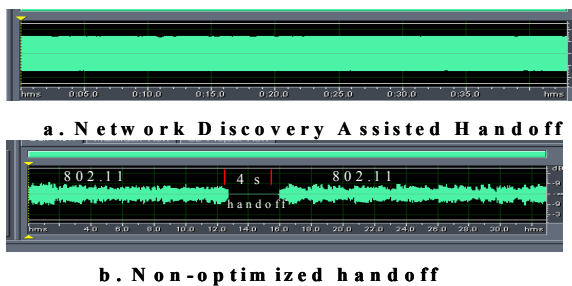


Figure 10. Effect of Network discovery aided handoff

Figure 10a and 10b compares the handoff results for network assisted mode and non-optimized mode respectively.

Network discovery assisted handoff reduces the handoff delay to 4 ms and achieves zero packet loss.

6 Conclusions

Efficient network discovery mechanisms provide the means for fast secured handoff by allowing the mobile to discover the network elements in the neighboring networks. We describe few techniques and elaborate several ways of

providing application layer network discovery scheme. These include both centralized and peer-to-peer models. We provide the details of the database format and the associated query mechanism used for the discovery. We describe how these techniques help provide proactive secured handoff during a mobile's movement between heterogeneous access networks and describe a specific implementation of network discovery assisted proactive handoff and its performance results.

7 References

- [1] E. Guttman, C. Perkins, J. Veizades, and M. Day, Service Location Protocol, Version 2, IETF RFC 2608, June 1999 <http://www.ietf.org/rfc/rfc2608.txt>
- [2] Sun Microsystems, Jini Connection Technology, <http://www.sun.com/jini>
- [3] Microsoft Corporation, Universal Plug and Play Device Architecture Version 1.0, June 8, 2000. http://www.upnp.org/UpnPDevice_Architecture_1.0.htm
- [4] Salutation Consortium, Salutation Architecture Specification Version 2.0c . Part 1, The Salutation Consortium, June 1, 1999 <http://www.salutation.org>
- [5] J. Hodges and R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", IETF RFC 3377, September 2002.
- [6] M. Liebsch, A. Singh, H. Chaskar, D. Funato and E. Shim, "Candidate Access Router Discovery," RFC 4066.
- [7] K. Arabshian and H. Schulzrinne, "GloServ: Global Service Discovery Architecture," First International Conference on Mobile and Ubiquitous Systems: Networking and Services.
- [8] RDF Primer, <http://www.w3.org/TR/rdf-primer>
- [9] Y. Ohba (Ed.) Protocol for carrying Authentication for Network Access (PANA), draft-ietf-pana-pana-10, IETF Draft, July 2005, Work in progress
- [10] D. Mitton et al, "Authentication, Authorization and Accounting Protocol Evaluation" RFC 3127
- [11] D. Harkins and D. Carrel, "Internet Key Exchange" RFC 2409
- [12] Jena Semantic Web Framework, jena.sourceforge.net
- [13] R. Droms, Dynamic Host Configuration Protocol, IETF RFC 2131, March 1997, <http://www.ietf.org/rfc/rfc2131.txt>
- [14] (XML), <http://www.w3.org/XML>
- [16] A. Dutta, Y. Ohba et al, "MPA assisted Proactive Handoff Scheme", ACM Mobiquitous 2005
- [17] J. Rosenberg et al, "RFC 3261", IETF
- [18] J. Arkko, B. Aboba, "Network Discovery and Selection Problem", draft-ietf-eap-netsel-problem-03, October 2005, Work in Progress, IETF
- [19] IEEE 802.11k Task Group, Radio Resource Measurement Enhancements, <http://grouper.ieee.org/groups/802/11/index.html>.
- [20] IEEE 802.11u Task Group, Interworking with External Networks, <http://grouper.ieee.org/groups/802/11/>