LEVERAGING ON NEIGHBOUR INFORMATION FOR OPTIMIZING NETWORK SELECTION

Jhoanna Rhodette Pedrasa[1] and Aruna Seneviratne[2]

[1] Electrical and Electronics Engineering Institute, University of the Philippines, Diliman, Quezon City, Philippines, e-mail: jipedrasa@upd.edu.ph

[2] Networks and Pervasive Computing Group, NICTA, Australia, e-mail: aruna.seneviratne@nicta.com.au

Received Date: July 11, 2014

Abstract

Current operating systems rely on Received Signal Strength (RSSI) to choose which network to connect. However, RSSI is not a good measure of actual network performance and requires the interfaces to be turned on, which can significantly drain the battery of the mobile node. This work revisits how network discovery is performed in a multi-radio, mobile environment. The current method of basing decisions on physical-layer characteristics cannot adequately capture network service parameters. Going beyond radio properties allows users to make better choices as to which is the "best" network and Point of Attachment to connect to. In this work we extend MOBIX, a system for managing MOBility using Information eXchange, which allows nodes to exchange information in a peer-to-peer manner in addition to leveraging on a centralized server. We performed simulations to study the performance of MOBIX with and without the map server and show that our enhanced system strikes a balance of providing a scalable, updated network performance information in densely populated areas and relying on a network server in less urbanized areas with lower number of nodes.

Keywords: Mobile devices, Multi-radio interfaces, Network discovery

Introduction

Multiple radio interfaces are the norm already in today's mobile devices. Even the most basic mobile smartphones have Bluetooth and WiFi aside from the cellular interface. We can expect that in the future, we see WiMax coexisting with Bluetooth, WiFi, and LTE.

Much of the work in heterogeneous networking has been focused on seamless hand-over between networks to ensure that QoS service guarantees are made. Such hand-over decisions hinge on discovering networks first, which have not received as much attention. Instead, each interface discovers available Points of Attachments (PoA) independently, requiring the interface to be turned on and thereby adding to the node's energy consumption. Furthermore, network discovery in current systems is based on radio signal properties. However, actual network performance is not dependent on radio characteristics alone. Throughput and delay vary according to factors such as usage patterns of other users and uplink bandwidth of the terminal. Thus, there is a need to look at network discovery in a multi-radio environment in a more integrated manner, and to use actual network performance as metric when making decisions on which PoA to use.

Discovering available networks and their associated performance metrics can be achieved through a variety of approaches. The node can estimate throughput or delay by actively injecting probe packets into the network. Prediction-based schemes build upon the regularity of user activities to anticipate future PoAs and their conditions. These schemes require a period of learning, and their performance deteriorate when users do not have fixed or discernable patterns or when they visit new locations.

The other option is to use the time-tested method of "asking our neighbors." We use networks to exchange data, why cannot we exchange information about the network?

Much as in real life where we ask the stranger when in unknown territories, we can ask the device nearby which network it is using and how much it costs. Sharing information with other nodes can be an effective and efficient means of discovering actual network performance metrics.

In our previous works [1,2] we present MOBIX, a system for managing MOBility using Information eXchange. MOBIX enables mobile devices to share network performance information with each other in a purely distributed manner using only the shortest-range interface (Bluetooth). Our results showed that MOBIX relying purely on reports from peers is effective for learning available networks and their performance. However, there will be instances when there are not enough nodes to generate and distribute reports. Under these conditions, it may be advantageous to leverage on data from a centralized map server instead. In this work, we extend MOBIX to incorporate a centralized entity in addition to the peer-to-peer functionality of mobile nodes. Our results show that the hybrid system outperforms server-only and peer-only based decisions, as it operates well in both instances of low map availability and low node density.

Literature Review

The problem of determining network availability beyond RSSI has been the subject of much research, particularly on IEEE 802.11 networks. It can be broadly classified into four categories according to method of discovery.

Self-discovered techniques determine available resources from the node's own measurements of current network conditions. A range of active bandwidth estimation tools are widely available already (e.g. [3,4,5]) but these were developed primarily for wired networks and do not perform well on wireless environments [6,7]. The work in [8] measured the timing delay of 802.11 management frames to estimate the load on the network, while [9] obtained the channel utilization ratio by observing the percentage of the time the node's radio is idle. Other approaches include approximating the contention level of the channel [10], counting the number of frame retransmissions [11], or sending modified probe packets [12]. These solutions, however, estimate only the maximum throughput a node can achieve on the wireless channel itself, and does not take into account uplink bandwidth to the rest of the Internet. Active measurements also require that the network interface be powered on to make measurements. In a multi-radio environment, having on multiple network interfaces can severely impact the battery life of the system. For instance, the HSDPA and WiFi interfaces have been found to be the top energy consumers on a smartphone when switched on [13].

Another approach is to use history-based solutions. This approach makes predictions by maintaining a record of past movement patterns of the device or a history of network metrics. For instance, Breadcrumbs [14] is an automatic AP discovery and selection system with a personal mobility model capable of generating connectivity forecasts from the device's movement patterns. Similarly, [15] used Dynamic Bayesian Model to predict WLAN availability from user context such as time of day, GSM location area, available WLANs, and number of Bluetooth devices found, while [16] predicted the probability that a user will have WiFi access and approximated the usage volume of each application type accessing the network based on past usage data. Prediction-based schemes require a period of learning however and will fail when users do not have discernible patterns at all or move to locations not visited before. Moreover, results in [17] revealed that it is difficult to predict precisely the timing of network handoffs when applied to WLAN data. Our system may be used to complement these soft prediction schemes, as MOBIX does not need any prior knowledge and can work in unfamiliar environments.

Network-assisted techniques require the APs to take an active role in disseminating network availability and performance information. In [18], every available AP sends it state information to the nodes through the beacon frame. The state information includes the number of associated stations, measured interference at the AP, and channel gain between the AP and the node. Luo, et al. [19] required APs to advertise the combined link date rates of mobile nodes already associated to it, similar to [20] which advocates broadcasting AP traffic load instead. Such techniques require modifications to the IEEE 802.11 protocol, thus it would not be backward compatible with existing infrastructure. Moreover, this technique implicitly assumes that APs and their administrators would be trustworthy enough to propagate reliable information. In a commercial environment, this may not be the case as it is actually at the operator's advantage to falsely advertise excellent network service to lure in more customers.

Finally, another approach to network availability involves collaboration among mobile devices. This method requires nodes to share network performance information with each other, which is then aggregated to build a network map, similar to what we are proposing. An example is "war-driving" operations, where users drive around a city or location logging AP radio signal parameters on a mobile computer. The logs are then made publicly available through sites such as Wigle [21] JiWire [22] and WeFi [23], providing users with maps of WiFi availability in an area. Similarly, WiFi-Reports [24] build a network map from data submitted by users while [25] investigates a cost-function-based network selection architecture assisted by a network map obtained from an MIIS service as defined in IEEE 802.21. Similar to the previous works above, MOBIX can leverage on a network server hosting the network maps. Network maps alone are fully dependent on a centralized server, however, which suffers from issues of scalability and fault-tolerance. Our system has the capability to perform in a decentralized manner and does not rely exclusively on a map server. These network maps, which have predominantly been for IEEE802.11 networks, can easily be extended to include data on other networks such as WiMax and GSM. Nodes can manage their energy resources more efficiently by pre-caching network maps or powering on a single interface to download the maps, which can include information on all possible interfaces.

System Overview

Network resource discovery beyond radio layer characteristics in wireless mobile environments is still an open problem. In this section, we present our enhanced system for managing MOBility using Information eXchange (MOBIX) that allows nodes to exchange information about network conditions with each other while still leveraging on a centralized server.

System Architecture

Figure 1 shows the over-all architecture of MOBIX. The system consists of the mobile nodes and two servers, a map server and a Certification Authority. Mobile nodes are portable computing devices (e.g. mobile phones, PDAs, Internet tablets, and notebook computers) that have multiple wireless interfaces. Mobile nodes generate reports on network conditions and upload these reports to the map server, which is tasked with aggregating reports into a network map. Additionally, nodes exchange reports with peers using a short-range communication channel such as Bluetooth, allowing them to work off-line when no network map or connection to the map server is available. As exchanging reports with peers may break the location privacy of nodes, the Certification Authority (CA) manages a token system to preserve user anonymity while still maintaining limited influence of nodes. In addition to privacy, the CA addresses the trust and security aspects of the system. A more detailed description of the security features of MOBIX can be found in [26].

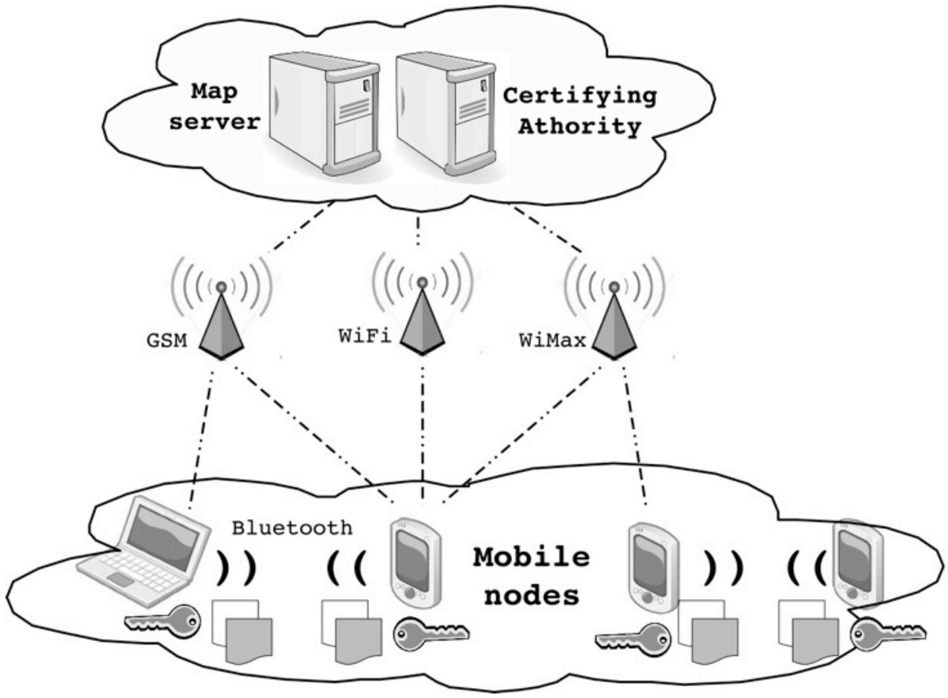


Figure 1. MOBIX system architecture

In brief, MOBIX works as follows. Nodes generate reports on network conditions at certain points in time and keep these reports in a data store. These reports are digitally signed using tokens issued by the CA, and are uploaded to the map server when a network connection is available. When a MOBIX node encounters another MOBIX node, they exchange reports from their data stores and uses the tokens to verify received reports. This peer-to-peer capability enables the nodes to make decisions in offline mode, if necessary.

When a mobile node wants to establish a network connection, the node searches its data store for relevant reports about available PoAs. It calculates the trustworthiness values of each relevant report and combines them into a single measure for every candidate PoA. The decision engine on the node then matches application requirements and user preferences with the combined network measure to allow the user to choose which PoA to use. If no relevant reports are found, the node attempts to download the map from the map server using whatever connectivity it has and makes a decision using the network map.

Node Architecture

A MOBIX node is a software agent executing on a user's device, which is actively gathering reports about network conditions from mobile peers it encounters. All mobile devices are potential MOBIX clients in our system. If not, beaconing may be incorporated to alert nodes of the presence of other participating nodes. When two or more MOBIX devices come within communication range they exchange reports with each other. The report contains the network conditions on all available interfaces experienced by a mobile node at a particular location and at a particular point in time. The main functions of a MOBIX node are shown in Figure 2.

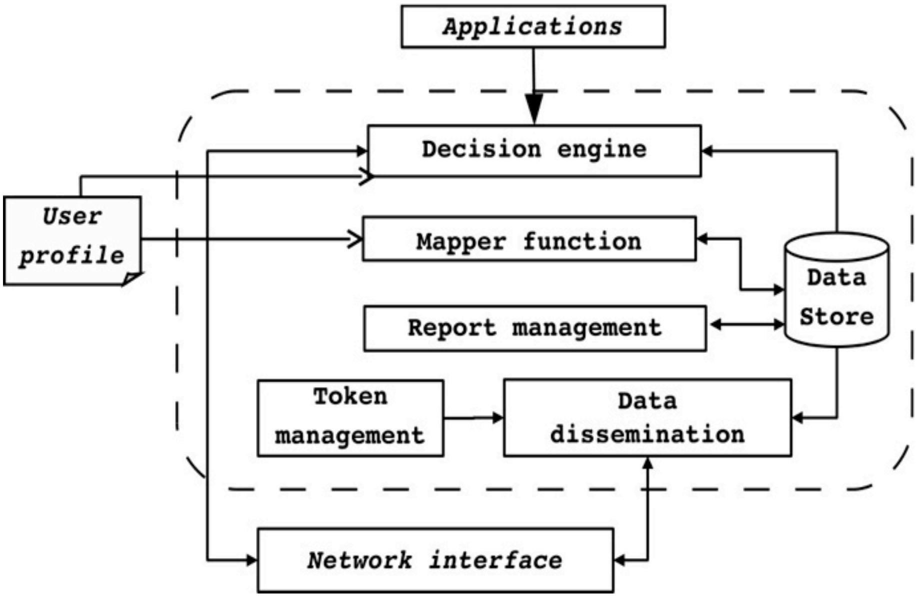


Figure 2. Modules in a MOBIX mobile node

The data store is where reports are stored and from which reports are chosen to be sent during an encounter. The data dissemination module decides when to transmit a report, which reports are sent, and implements the communication protocol used to exchange reports between mobile nodes. The report management module maintains the data store on each mobile node. It determines when a new report is generated by the node (if it is a generator node), which received reports to insert into the data store, and how reports are deleted.

The token management module implements the security protocol of the node. In particular, it manages the public/private key pairs and determines which key to use in signing messages and the corresponding token to attach.

The mapper module aggregates received reports in both space and time. It maps the raw data into a meaningful quality measure for use by the decision engine, such as RSSI to predicted throughput. Finally, the decision engine takes the user profile and application requirements and tries to match it with available network resources using information gathered in the data store. It aggregates relevant reports and reconciles conflicting data using a data fusion technique. It then makes a decision on which interface and PoA to use.

In our previous works, we showed by simulation that MOBIX is effective for network resource discovery while operating purely in a peer-to-peer environment. The interested reader is referred to [1] which describes the mobile node peer-to-peer functionality in greater detail, focusing on report management, data dissemination, data integrity and the decision engine.

Server Architecture

Our current work builds upon the peer-to-peer functionality by introducing centralized entities. There are two servers in the system, namely the Certifying Authority (CA) and the map server. Although in practice these would likely reside on the same machine, they perform two different functions and should thus be logically treated separately. The CA is tasked with generating the tokens and the corresponding public/private key pairs and also manages the revocation list. The map server generates the QoS maps from the reports submitted to it by users. Figure 3 shows the different components of these two servers.

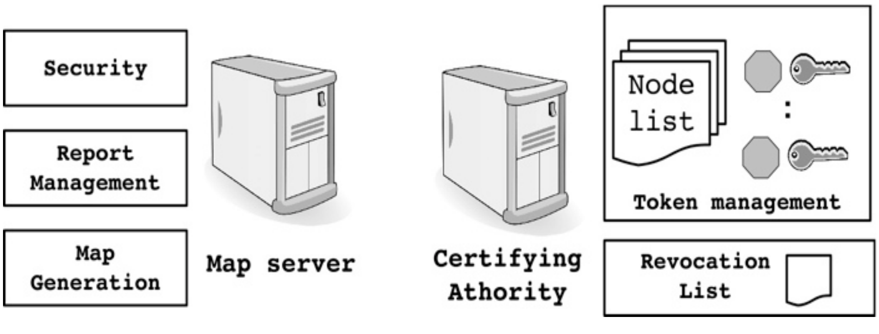


Figure 3. Modules in the map server and certifying authority

The network map server aggregates the reports submitted by nodes and represents the QoS of network points of attachments in a given area or zone. Each entry in the map corresponds to aggregated reports for PoAs available at a particular physical location. The security module on the map server implements the security algorithms needed to verify tokens and digitally signed reports. It also keeps a revocation list to filter out messages from unauthorized and revoked nodes. The report management module performs the rate-limiting function of the map server, should it be found desirable to limit the rate at which individual nodes can submit reports. Reports are inserted into the corresponding vector entry and an aggregation mechanism is employed by the map generation module to update the map. More sophisticated algorithms can also be used to better predict future values from historical data.

The CA is a trusted server tasked with generating the public/private key pairs and corresponding tokens needed by the mobile nodes. These tokens are pseudonymous digital certificates signed by the CA, allowing mobile nodes to verify reports from peers even when the CA is offline. Each mobile node is issued a set of tokens but only one can be used at any given time. These tokens are refreshed periodically to ensure the location privacy of mobile nodes from peers.

In the next sections we give more detailed descriptions and evaluation of the map server in the system.

Leveraging on a Server

We have shown from our previous works that MOBIX relying on reports from peers is effective for learning network availability and performance. However, there will be instances when there are not enough nodes to generate and distribute reports. Under these conditions, it may be advantageous to leverage on data from a centralized map server instead. In this section we discuss in detail the hybrid MOBIX system, focusing on the centralized map server for managing network maps in addition to the peer-to-peer functionality of mobile nodes.

Map Server and Mobile Node Overview

Figure 4 gives an overview of the map server and mobile node interaction. Mobile nodes in MOBIX upload reports to a centralized map server in addition to distributing reports directly to peers. Reports generated by nodes are concatenated and submitted to the map server at less frequent intervals (e.g. every 10 minutes as opposed to every 5 sec when transmitting to peers) when the node has a network connection. The map server aggregates the reports to build a network map that is made available to mobile nodes.

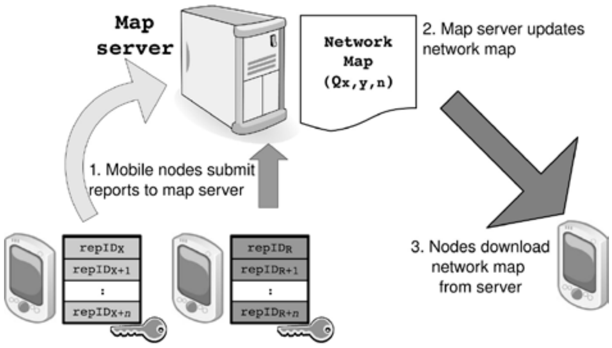


Figure 4. Overview of the map server and mobile node interaction

When attempting to make a network connection, the mobile node checks its data store for relevant reports. If relevant reports are found, it proceeds as in the peer-based system discussed in [1]. Otherwise, if no relevant reports are found, the node attempts to access a network map from the map server. This is possible if, for instance, the user has a paid subscription to a map service with its own dedicated network which subscribers can access for the sole purpose of downloading network maps. Alternatively, network operators can also provide this service for free to promote load balancing among their various APs.

MOBIX nodes have the option to pre-cache and download network maps from the server before traveling. In this case, the node checks first that the map entry is still valid. If the map was generated more than *X* time periods ago, the node contacts the map server again to check for an updated map.

Network Map

The main function of the map server is to aggregate reports and build the network map. The network map is created as a matrix *Q* with *x* rows, *y* columns, and depth *n*. The entry $Q_{x,y}$ corresponds to a physical area (x,y) in the map and the third dimension *n* lists all the network PoAs available at that location. Mobile nodes submit reports to the map server to update the entry of vector Q corresponding to the physical location where it was generated. These reports are then aggregated to form $Q_{x,y,n}$ for each zone.

The map server builds the network map by updating the corresponding entry in Q as reports come in. The simplest method to summarize the reports for PoA n at location (x,y) is to get the weighted average of the report, eg

$$< M_{t,n} > = \frac{\sum w_{R,k} \cdot M_{R,n}}{\sum w_{R,k}}, \forall R: dist \ < \ d_{max}$$

where $w_{R,k}$ is the trustworthiness value of report *R* and $M_{R,n}$ is the corresponding reported network measure value of *R* on PoA_n.

Averaging can be significantly skewed by a small fraction of outliers however, making the system susceptible to attacks by malicious report-generating nodes. Our work in [27] explored four data fusion techniques, namely average weight, weighted function, Bayesian inference, and Dempster-Shafer Theory. Our results show that there is no clear choice as to which data fusion technique is optimal for our system as each one has its strengths among the different evaluation scenarios explored. We concluded that Dempster-Shafer Theory is the most promising as it is robust to attacks across a wider range of trustworthiness values compared to averaging and weighted function, and is less sensitive to errors in trustworthiness calculations than Bayesian inference.

Mobile nodes can pre-cache network maps before traveling, or download them only when it needs to make a network connection. An entry in the map lists all the network PoAs accessible within the vicinity of the node's location as shown in Table 1.

Table 1. Contents of an Entry in the Network Map

Variable	Description
PoA_n	PoA name
Op_n	Operator owning or administering PoA_n
C_n	Cost of connection through PoA_n
$M_{x,y,n}$	combined network measure for PoA_n at location (x,y)
$N_{x,y,n}$	number of reports contributing to $M_{x,y,n}$
t_n	timestamp of when $M_{x,y,n}$ was last updated

Each entry includes information on the name, operator and associated cost of connecting through this PoA, as well as the aggregated measure, the number of reports contributing to this aggregate, and the timestamp of when this value was last updated. The network map is thus a collection of these entries corresponding to a physical area or location the mobile node is interested in.

Mobile Node

Reports in MOBIX are generated either periodically or when an event occurs. These reports are submitted to the map server whenever a network connection becomes available. Reports distributed to peers are signed individually (per report) and are transmitted periodically to peers at intervals ranging between 5 sec to 60 sec in our simulations. In contrast, reports are submitted in bulk to the map server to optimize the process. Reports are first buffered on the mobile nodes and when the buffer becomes full (e.g. the node has generated 10 reports), these reports are concatenated and sent to the map server. Nodes only submit reports that they themselves produced; that is, they do not submit reports received from other nodes. This is to ensure that a report will be submitted just once to the server, eliminating duplicate submissions. Mobile nodes encrypt reports first before sending them to the server over a secure connection to protect their messages from being intercepted by eavesdroppers.

Nodes can opt to perform pre-caching by downloading network maps while it still has a network connection, in anticipation of it moving to a new location. Note that MOBIX nodes operating in peer-to-peer mode make decisions using reports that were generated in the past few minutes. On the other hand, pre-caching maps means that by the time the node accesses the map, the information could be stale already and do not correctly reflect current network conditions.

Figure 5 shows the flowchart of the decision process at the mobile node. When a node has to make a network connection, it first checks its data store for relevant reports which are still valid, e.g. generated within the last *X* seconds. If so, it uses the reports from the data store to make a decision. Otherwise, the node checks the timestamp of the pre-cached map, if it is available. If a pre-cached map exists and it is still valid, the node bases it decision on the map. Otherwise, it attempts to contact the network map server to download an updated map. This process reflects that reports received from peers take precedence over the network map as it presents more recent information.

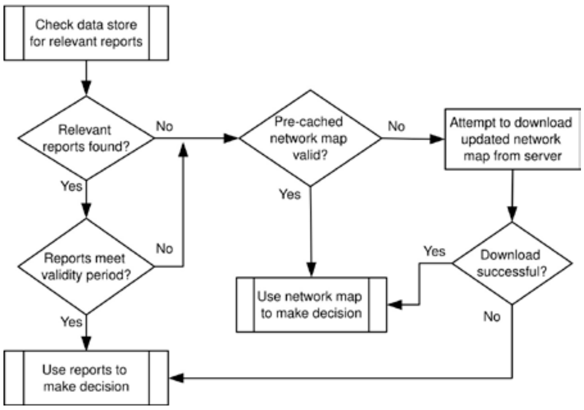


Figure 5. Flowchart of the decision process on the mobile node

Map Server

We assume that the map server is trustworthy at all times and that it is required to take measures to protect reports and preserve the location privacy of nodes. This could be achieved by strong legislation similar to the Telecommunications Privacy Law in Australia [28] or the Electronic Communications Privacy Act [29] in the U.S.A., which obligates telecommunications carriers and service providers to protect the privacy and personal information of telecommunications users. Privacy information can be secured by stripping device specific information like IP addresses before passing them on to the map server application.

The map server may wish to limit the rate at which mobile nodes can submit reports about a particular PoA or a particular location. This is to ensure that a malicious node will not be able to manipulate the aggregated network measure by simply sending a large number of reports. This could be achieved by keeping track of the number of reports submitted by each user over a period of time and discarding new reports submitted by nodes exceeding the set limit.

Evaluation

We evaluate the impact of a map server by simulation using Network Simulator 2 (NS2) with the NS Miracle plug-in. Each MOBIX node has two interfaces. One interface emulates a Bluetooth interface with a 10m-transmission range. The other interface is an 802.11b WiFi interface with a transmission range of 100m. We fixed the simulation area to 500 x 500 meters[1], divided it into four equally sized quadrants, and placed an Access Point (AP) at the center of each quadrant. Two of the APs have a high-bandwidth connection to an FTP server, while the other two have low bandwidth connections to the same FTP server. About 73% of the simulation area has WiFi coverage, thus there are pockets in the simulation area where there is no available WiFi network. Table 2 lists the position of the APs on the simulation area and the uplink bandwidth to the FTP server.

There are two types of MOBIX nodes in the simulation. Generator nodes periodically create reports about the throughput of their active network connections and distribute these reports to other nodes over the Bluetooth interface. Forwarder nodes, on the other hand, do not generate reports but simply forward reports received from other nodes periodically.

[1] Without loss of generality, we used a simulation area of 500m x 500m as the results depend on the node density as opposed to the physical size of the simulation area

We fix the number of mobile nodes to 250 nodes in our simulations for an effective population density of 1,000 nodes per km^2, which approximates medium-to-high density cities such as Tokyo. Of the 250 nodes, only 20% are generator nodes and the rest are forwarder nodes. Each node can cache up to 200 reports in its data store, and sends only the top 20% (or 40 reports) periodically every 15 sec.

Table 2. Settings of Access Points in the Simulation Area

AP name	Position(x,y)	Uplink Bandwidth to FTP server
AP0	(125,125)	1 Mbps
AP1	(375,125)	0.5 Mbps
AP2	(375,375)	1 Mbps
AP3	(125,375)	0.5 Mbps

Nodes start moving when the simulation starts (t = 0) and after 5 minutes, a forwarder node attempts to transfer a 1MB file to the FTP server over the WiFi interface. The node searches its data store for relevant reports, and if no reports are found it attempts to use the network map instead. The node executes a file transfer every minute and the simulation ends after 25 attempts. Each scenario is tested using 200 simulation runs with a unique movement file per run, and the results averaged at 95% confidence interval.

Three mobility models were used in the simulations, namely Random Waypoint [30], Manhattan Grid [31], and Self-similar Least Action Walk [32] models. These models were chosen as they represent diverse mobility patterns. Random Waypoint (RW) and Manhattan Grid (MG) are well-known synthetic mobility models used by the MANET community for analyzing routing protocols [33]. These are purely synthetic models however, and do not exhibit statistical patterns of real human walks [34]. The third mobility model addresses this issue. Self-similar Least Action Walk (SLAW) is a trace-based mobility model able to produce synthetic walk traces with truncated power-law distribution of flights, pause-times and inter-contact times, fractal way-points, and heterogeneously defined areas of individual mobility. Though not as well known, SLAW creates more realistic human mobility patterns than RW and MG. Table 3 summarize the parameters used when the movement files were generated using the mobility models.

Table 3. Node Movement Parameters

Variable	Value
General Parameters	
Mean node speed	1.9 m/sec
Mean pause time	15 sec
Simulation area & time	500x500m, 1800 sec
Manhattan Grid parameters	
Number of blocks	5x5
Turn probability	0.5
Seconds ignored	first 1800 sec
Self-similar Least Action Walk parameters	
Distance alpha	1.5
Number of waypoints	500
Hurst parameter	0.75
Clustering range	25 m
Levy exponent for pause time	1

We set the probability of connecting to the higher throughput network, *P(high throughput)*, as our evaluation criteria. We counted the number of times the forwarder node was able to connect to the higher throughput network for the duration of the simulation. More formally, the probability of the forwarder node choosing the high throughput network is defined as

$$P(high\ throughput) = \frac{Number\ of\ times\ connected\ to\ high\ throught\ network}{Total\ number\ of\ file\ transfer\ attempts}$$

We assume that nodes do not perform pre-caching of network maps, which means the node must first attempt to fetch the map from the server if no relevant reports are found every time it needs to determine which AP to connect to. This probability of network map being available, denoted as *pMap*, takes into account that there is a network connection to the map server, the map server is up, and there is a relevant map corresponding to the user's current location. As these are independent events, *pMap* is modeled as

$$pMap = f_{N,S,M} = f_N(n)\cdot f_S(s)\cdot f_M(m)$$

where $f_N(n)$, probability density function (pdf) of a network connection from the mobile node to the map server

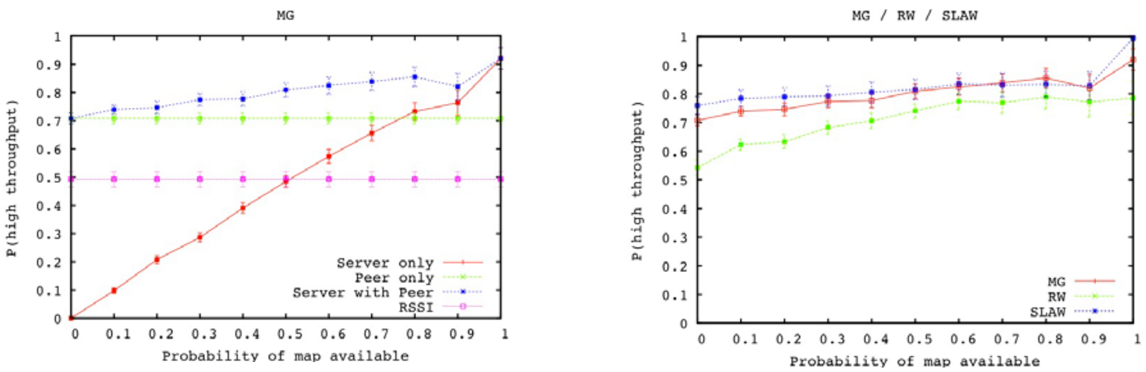
$f_S(s)$, pdf of map server availability

$f_M(n)$, pdf of relevant network map being available

We use the uniform probability distribution to vary *pMap* with respect to the mobile node in the simulations. This allows us to explore the efficiency of the hybrid system across a wider range of scenarios. The actual value of *pMap* will depend on various factors such as how diligent the node is in pre-caching maps, the validity period it sets, and whether it has a subscription to a network map service.

Results

Figure 6 shows the probability of connecting to the high throughput network at varying probability of map available, *pMap*. In the figure, “Server only” denotes the case where the node is fully dependent on the map server and is unable to make a network connection when no map is available. "Peer only" presents the results for a MOBIX node purely relying only on reports from peers while "Server with Peer" is the hybrid system where the node uses both the network map and reports received from peers to make a decision. For comparison, we plot "RSSI" as the baseline case where the node chooses the PoA with the strongest signal strength.



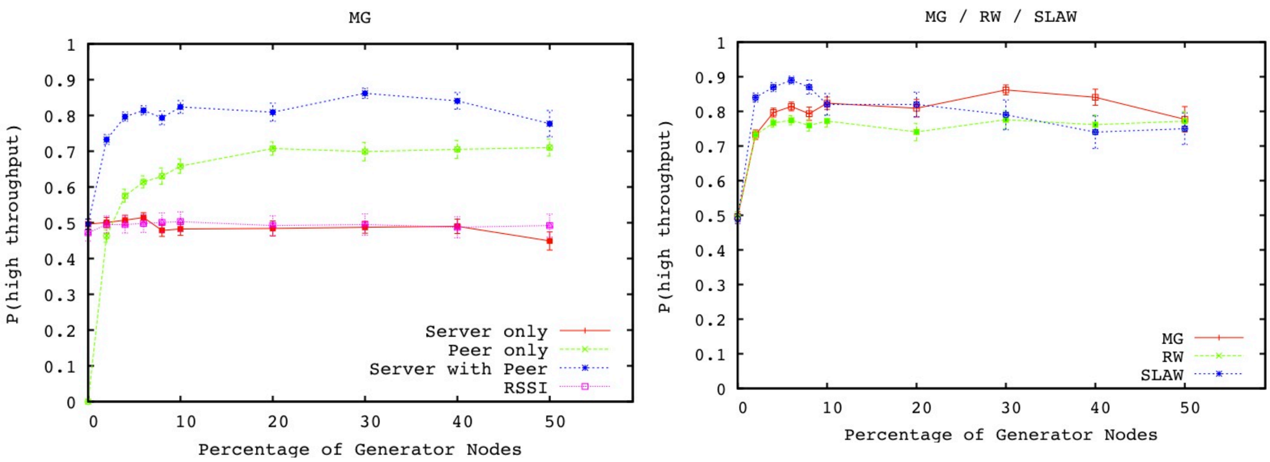
(a) Manhattan grid (MG)

(b) MG / RW / SLAW

Figure 6: Effect of varying probability of map available (pMap) on the probability of connecting to high throughput network

It can be seen from Figure 6 that our hybrid system using both a map and the peer-to-peer components outperforms server only, peer only, or RSSI based decisions. The probability for the node to connect to the high throughput network is 0.5 using RSSI in the Manhattan Grid model (Figure 6(a)). By relying on reports from peers, this probability goes up to 0.7, an improvement of about 40% over RSSI-based decisions. With the network map and peer-to-peer capability, the value further increases to 85% of the time. Note that the baseline case (RSSI) is independent of the probability of map available, while the "Server only" case is fully dependent on the value of *pMap*. It can also be seen from Figure 6(b) that we get similar results using MG and SLAW as mobility models while RW can be considered the performance in the worst-case scenario.

Figure 7 plots *P(high throughput)* at varying percentage of generators, keeping the number of nodes constant at 250 and *pMap* at 0.5. Figure 7(a) shows that even at low percentage of generators (less than 10%), MOBIX utilizing both the network map and peer reports outperforms server-only, peer-only and baseline RSSI results. The probability of choosing the high throughput network is around 0.8 using the map server with peer, compared with 0.7 for peer only and 0.5 for both server-only and RSSI. The number of nodes is sufficiently large that even the peer-only MOBIX outperforms relying on RSSI or the server only.



(a) Manhattan grid (MG) (b) MG / RW / SLAW

Figure 7. Effect of varying percentage of generator nodes (pGen) on the probability of connecting to high throughput network

The results show that hybrid MOBIX using both map server and peer reports strikes the optimal balance between map availability and population density. A purely server-based approach requires a network connection in order to download the most up-to-date map. This presents a chicken-or-egg problem that necessitates the node to have a network connection first in order for it to make the optimal decision on which network to connect to for the actual data transfer. Pre-caching maps would be the obvious solution, but this requires the user to plan ahead or for the node to predict the user's future locations. On the other hand, a purely peer-based approach requires the cooperation of a large number of nodes in order to be feasible.

Hybrid MOBIX outperforms the server-only and peer-only approach in both instances of low map availability and low node population density. The hybrid system allows nodes to get timely information from peers and leverage off a centralized network map when needed. This comes at a cost of additional complexity on the mobile nodes. Much of the processing overhead lie in managing the data store and in the network connection, both for distributing reports to peers and for connecting to the map server to submit reports and download the map. In terms of energy cost however, using a short-range communication channel such as Bluetooth allows significant energy savings [2]. Additionally, nodes submit reports to the map server only when a network connection is present.

Mobile devices of today are more advanced than the average desktop computers a decade ago. Chip technology is continuing to progress at the rate dictated by Moore's law, allowing for the production of faster, more energy-efficient processors. These developments in technology will lessen the impact of the additional complexity incurred by our system. Additionally, enabling mobile devices access to network metrics ultimately translates to improved user experience.

Conclusions

There is a need to rethink the manner by which wireless networks are being discovered. Current mobile devices are heavily reliant on radio signal properties, which lead to inefficiencies in managing the system in terms of energy and decision-making. In this work we build upon MOBIX, an integrated approach to network discovery that uses the lowest-energy interface to learn about the conditions of the other wireless interfaces by exchanging information with peers.

MOBIX relying on peers for reports require the cooperation of a sufficient number of nodes, however. To address the cases where node density is low, this paper explores the inclusion of a centralized map server that can provide a network map to the nodes. We have shown by simulations that MOBIX leveraging on a map server aside from reports from peers outperform server-only and peer-only based decisions, as it operates well in both instances of low map availability and low node density. By trading off processing complexity to robustness and efficiency, our hybrid approach addresses the problem of fault tolerance of a centralized solution while still providing acceptable performance when the number of peers is insufficient.

References

[1] J.R. Pedrasa, and A.P. Seneviratne, “Mobix: System for managing mobility using information exchange,” In: *Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous ’09)*, IEEE, pp. 1–10, 2009.

[2] J.R. Pedrasa, M.A. Pedrasa, and A.P. Seneviratne, “Information exchange for enhanced network selection,” In: *Wireless Communications and Networking Conference (WCNC)* 2010, IEEE, pp. 1-6, 2010.

[3] N. Hu, and P. Steenkiste, “Evaluation and characterization of available bandwidth probing techniques,” *IEEE Journal on Selected Areas in Communications*, Vol. 21, No. 6, pp. 879–894, 2003.

[4] E. Goldoni, and M. Schivi, “End-to-end available bandwidth estimation tools: An experimental comparison,” In: *Second International Conference on Traffic Monitoring and Analysis (TMA '10)*, Springer-Verlag, pp. 171-182, 2010.

[5] C. Leong, T. Wei, A. Samsudin, and A. Bandi, “Performance evaluation of optimized available bandwidth estimation tools in FTTH networks,” In: *2012 18th Asia-Pacific Conference on Communications (APCC)*, IEEE, pp. 221-226, 2012.

[6] D. Gupta, D. Wu, P. Mohapatra, and C. Chuah. "Experimental comparison of bandwidth estimation tools for wireless mesh networks," Paper presented at *IEEE INFOCOM Mini-conference 2009*, April 2009.
[7] H. Lee, V. Hall, K. Yum, K. Kim, and E. Kim. "Bandwidth estimation in wireless LANs for multimedia streaming services," *Advances in MultiMedia*, Vol. 2007, No. 1, pp. 9–9, 2007.
[8] P.A.K. Acharya, A. Sharma, E.M. Belding, K.C. Almeroth, and K. Papagiannaki, "Rate adaptation in congested wireless networks through real-time measurements," *IEEE Transactions on Mobile Computing*, Vol. 9, No. 11, pp. 1535 -1550, 2010.
[9] Y. Peng, Y. Yu, L. Guo, D. Jiang, and Q. Gai, "An efficient joint channel assignment and QoS routing protocol for IEEE 802.11 multi-radio multi-channel wireless mesh networks," *Journal of Network and Computer Applications*, Vol. 36, No. 2, pp. 843-857, 2013.
[10] H. Lee, S. Kim, O. Lee, S. Choi, and S. Lee, "Available bandwidth-based association in IEEE 802.11 wireless LANs," In: *11th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2008*), ACM, New York, United States of America, pp. 132–139, 2008.
[11] J. Jang, Y. Lim, and C. Kim, "Traffic-aware decentralized AP selection for multi-rate in WLANs," In: *12th International Conference on Advanced Communication Technology (ICACT 2010)*, IEEE, pp.278 - 283, 2010.
[12] F. Xu, C. Tan, Q. Li, G. Yan, and J. Wu. "Designing a practical access point association protocol," In: *IEEE International Conference on Computer Communications (INFOCOM 2010)*, IEEE, pp. 1–9, 2010.
[13] G. Perrucci, F. Fitzek, and J. Widmer, "Survey on energy consumption entities on the smartphone platform," In: *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, pp.1-6, 2011.
[14] A. Nicholson, and B. Noble, "BreadCrumbs: forecasting mobile connectivity," In: *14th ACM International Conference on Mobile Computing and Networking (MobiCom '08)*, ACM, New York, United States of America, pp. 46–57, 2008.
[15] U. Rathnayake, M. Ott, and A. Seneviratne, "A DBN approach for network availability prediction," In: *12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '09)*, ACM, New York, United States of America, pp. 181–187, 2009.
[16] Y. Im, C. Joe-Wong, S. Ha, S. Sen, T. Kwon, and M. Chiang. "AMUSE: empowering users for cost-aware offloading with throughput-delay tradeoffs," In: *IEEE International Conference on Computer Communications INFOCOM 2013*, IEEE, pp. 435 - 439, 2013.
[17] L. Song, U. Deshpande, U.C. Kozat, D. Kotz, and R. Jain, "Predictability of WLAN mobility and its effects on bandwidth provisioning," In: *25th IEEE International Conference on Computer Communications (INFOCOM 2006)*, IEEE, pp. 1–13, 2006.
[18] W. Ge, S. Chen, H. Ji, X. Li, and V. Leung, "Green access point selection for wireless local area networks enhanced by cognitive radio," *Mobile Networks and Applications*, Vol. 18, No. 4, pp. 553-566, 2013.
[19] L. Luo, D. Raychaudhuri, H. Liu, M. Wu, and D. Li, "End-to-end performance aware association in wireless municipal mesh networks," In: *IEEE GLOBECOM Workshops*, IEEE, pp. 1–6, 2007.
[20] N. Papaoulakis, and C. Patrikakis, "A proactive, terminal based best access point selection mechanism for wireless LANS," In: *2008 IEEE GLOBECOM Workshops*, IEEE, pp. 1–4, 2008.

[21] "WiGLE:Wireless Geographic Logging Engine," (n.d.) [Online]. Available: http://www.wigle. net/ [Accessed: July 9, 2014]
[22] "Jiwire Global Wifi Finder," (n.d.) [Online]. Available: http://v4.jiwire.com/search-hotspot-locations.htm [Accessed: July 9, 2014]
[23] "WeFi," (n.d.) [Online]. Available: http://www.wefi.com. [Accessed: July 9, 2014]
[24] J. Pang, B. Greenstein, M. Kaminsky, D. McCoy, and S. Seshan, "Wi-Fi reports: Improving wireless network selection with collaboration," In: *7th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '09),* ACM, New York, NY, USA, pp. 123–136, 2009.
[25] H. Liu, C. Maciocco, V. Kesavan, and A. Low, "Energy efficient network selection and seamless handovers in mixed networks," In: *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops, 2009.* WoWMoM 2009, pp.1-9, 2009.
[26] J.R. Pedrasa, and A.P. Seneviratne, "Distributed network resource discovery on a mobile device," In: *IEEE Region 10 Conference 2012* (TENCON 2012), IEEE, pp.1,6, 19-22, 2012.
[27] J.R. Pedrasa, and A.P. Seneviratne, "Determining network availability on the move," In: *2011 17th Asia-Pacific Conference on Communications (APCC),* IEEE, pp. 301–306, 2011.
[28] Protection of Communications: Telecommunications Act 1997, [Online]. Available: http://www.efa.org.au/Issues/ Privacy/ta.html
[29] Electronic Communications Privacy Act of 1986 (ECPA), [Online]. Available: http://it.ojp.gov/default.aspx?area=privacy &page=1285
[30] D. Johnson, and D. Maltz, "Dynamic source routing in ad hoc wireless networks," In: T. Imielinski, and H. F. Korth, eds., *Mobile Computing*, Vol. 353 of The Kluwer International Series in Engineering and Computer Science, Springer, United States, pp. 153–181.
[31] F. Bai, N. Sadagopan, and A. Helmy, "The important framework for analyzing the impact of mobility on performance of routing protocols for Ad Hoc networks," *Ad Hoc Networks*, Vol. 1, No. 4, pp. 383 – 403, 2003.
[32] K. Lee, S. Hong, S.J. Kim, I. Rhee, and S. Chong, "SLAW: A new mobility model for human walks," In: *28th IEEE Conference on Computer Communications (INFOCOM 2009),* IEEE, pp. 855-863, 2009.
[33] F. Ros, P. Ruiz, and A. Gomez-Skarmeta, "Performance evaluation of existing approaches for hybrid ad hoc networks across mobility models," In X. Jia, J. Wu, and Y. He, eds., *Mobile Ad-hoc and Sensor Networks*, Vol. 3794 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp. 886-896, 2005.
[34] M. Musolesi, and C. Mascolo, "Mobility models for systems evaluation," In B. Garbinato, H. Miranda, and L. Rodrigues, eds., *Middleware for Network Eccentric and Mobile Applications*, Springer Berlin Heidelberg, pp. 43–62, 2009.