ProxNet: 近接センシングによるワイヤレス環境制御のための直接操作技法

ProxNet: A Direct Manipulation Technique for Dynamic Wireless Networking

暦本 純一　味八木 崇　河野 通宗[*]

Summary. This paper presents a new interaction technique for establishing ad-hoc and infrastructure wireless networks based on ”physical proximity”. Users can establish a securely wireless connection between two digital devices by simply put them together and press a connection button. Then, those devices identify one another by measuring radio-signal strength of received packets. We designed a set of protocol that supports exchange of a one-time session key and thus the resulting network connection is kept secret. We also introduce a notion of ”dummy point” which is the analogous of wireless access point but only deals with proximity communication mode for network session establishment. The dummy point can also represent physical locations or objects, allows a user to get context-sensitive interactions.

1　はじめに

デジタル情報機器，特に IEEE802.11 や Bluetooth などの無線ネットワークを装備したデジタル機器が急速に普及している．これらの無線技術によって，情報機器の利用形態は，従来の有線ネットワークの時代とは異なったものになる．有線ネットワークでは，機器の接続関係は静的であり，一定の場所で長く機器を使う利用形態が普通だった．無線を利用した機器では，ネットワークの接続関係は利用者の移動や作業内容に対応して動的に変化する．たとえば，以下のような利用形態が一般的になるであろう．

- 街で出会った友人とデジタル写真を交換する．友人の PDA と自分のデジカメを無線で接続し，画像ファイルを転送する．また，お互いの機器の画面を共有して，どのファイルを交換するかなどをインタラクティブにきめていく．
- 街頭キオスクから自分のデジタル機器に情報を取得する．
- カフェでホットスポットに接続．さらに同席した相手とファイルの交換を行なう．（ただし，同じホットスポットに接続している他のユーザに通信が盗聴されないようにしたい）
- 複数の携帯ゲーム機器の間でアドホックに無線ネットワークを形成して，対戦ゲームをはじめる．
- 会議室のスクリーンを使ってプレゼンテーションを行なう．スクリーンに対応するコンピュータと，会議室に持ち込んだ携帯型コンピュータとは無線によって接続する．（ただし，携帯型コンピュータをこの会議室に持ち込むのは今回が初めて．）
- オフィスにある公共ディスプレイに写真をアップロードする．

このような利用形態では，利用者は機器間の接続関係を状況・目的に応じて頻繁に切り替えるので，接続に際してのユーザインタフェースが重要になる．[1] われわれは，以下の二つの課題がとくに重要であると考えている．

機器の指定: ワイヤレス環境では，利用者が携帯機器を持ち歩き，その場で動的に接続を開始したい場合が多い．通常のネットワークでは対象機器はホスト名や IP アドレスなどの識別子を使うが，たとえば自分の目の前にあるプリンタのアドレスがわからない場合，手作業でそれを調べるのは非常に煩雑である．そもそも，まずネットワークに接続しないと調べることが不可能な場合もあり得る．

通信の安全性: さらに，ワイヤレス接続のユーザインタフェースで課題となるのは安全性と簡易性の両立である．現状の 802.11 では，SSID や MAC アドレスによる制限，WEP キーによる暗号化が提供されているが，WEP キー自体の暗号強度の問題に加えて，同じワイヤレス環境の利用者全員で共通の鍵

[*] Jun Rekimoto, Michimune Kohno ソニーコンピュータサイエンス研究所インタラクションラボラトリ, Takashi Miyaki 東京大学

[1] 本論文では,「接続」という用語を，ネットワーク層での接続と，アプリケーション層での接続（サービスの連携）とを含む意味で用いる．たとえば，Bluetooth や，IEEE802.11 のアドホックモード接続では，データ通信に先立って二者間での相互機器特定・認証などの手続きを経て「接続」を確立する必要がある．一方，802.11 のインフラストラクチャー・モードでは，機器がすでにアクセスポイントに接続している状態で，たとえば目前にあるプリンタに対して印刷データを送信したい場合がある．この場合，プリンタの IP アドレスなどのアドレス情報の取得や，プリンタにアクセスするためのアクセス権の取得が必要になる．これはアプリケーション層におけるネットワークサービスの「接続」である．一方，利用者からみると，どちらも「複数の機器を接続して目的の作業を行なう」ように見える．

を使うといったアーキテクチャー上の問題が指摘されている．

一方，WPA や IEEE802.1x のように，各利用者ごとに証明書を発行して公開鍵暗号系を用いたチャレンジ認証を行なう方式が普及しつつある．認証の安全性は高くなるが，事前に設定すべき情報も多くなる．静的なワイヤレス環境での利用にはよいが，動的な利用形態では証明書の発行や管理の作業が問題となる．たとえば街で出会った二人の間で，機器間に一時的に安全なワイヤレス通信路を確保する，といったアドホックな利用形態では，実際の通信に先立っての煩雑な設定作業が必要になってしまう．

1.1 物理的な位置関係を利用したワイヤレス制御

これらの課題の背景には，ワイヤレス環境へのアクセス方法を，従来の静的なネットワーク環境の延長としてとらえている点にあると考える．実際には，携帯ワイヤレス機器の利用形態は，遠隔地の機器と機器を接続する場合に留まらず，利用者の周辺にある，比較的近距離の機器間での接続である場合が多い．したがって，アドレスや機器名などの間接的な表現ではなく,「このプリンタ」というように機器を直接的に指定できたほうがはるかに直感的である．筆者らは，これらの発想に基づいて，図 1 に示すようなワイヤレス接続向けのユーザインタフェースをこれまでに提案してきた [2, 6, 1, 5].

方式	利用者操作	必要な機器
a. RFID[6]	機器の接近	非接触タグ タグリーダー
b. 赤外線 [6]	機器 A を 機器 B に向ける	赤外線 送受信器
c. 目視 [1]	機器 A に表示された 番号を機器 B に入力	A に表示装置 B に入力装置
d. 同期操作 [5]	機器 A と機器 B で 同期した操作 (ボタン同時押し等)	ボタン等

図 1. 近傍の機器を接続するためのユーザインタフェース

これらの方式の共通の発想は，機器を特定する手段として，機器間の位置関係を重視している点である．たとえば方式 a では，２台の機器を接近させることで接続する機器を特定している．方式 b では，1 台目の機器から赤外線ビームを接続対象となる機器に向けて発射する．セッションが確立された後は，通常のワイヤレス通信によって実際のデータを送受する．利用者には「機器と機器を近づけたり，目的の機器に向けてればネットワーク接続が確立される」という直接感のある操作を提供している．

しかし，これらの方式では，通常のワイヤレス通信手段のほかに，赤外線送受信部や非接触タグリーダなどの付加的なハードウェア・通信手段が必要であった．また方式 c や d は，利用者の目視に頼ったり，両手で同時に両方の機器のボタンを押すといった付加的な操作が必要だった．

2 信号強度計測によるネットワーク制御

本論文では，ワイヤレス通信における受信パケット信号強度を計測することで，近傍にある機器からの発信を特別扱いし，ネットワークの設定に利用する方法を提案する (図 2).

具体的には，利用者が 2 台の機器間での安全なネットワーク・セッションを確立したい場合には，単に 2 台の機器を接近させて「接続ボタン」を押す．この操作で発信される接続要求パケットは，信号強度を測定して，近傍の機器のみが接続要求に反応するようになっている．このようにして接続の設定が完了すると，通常のワイヤレス通信が利用可能なので，2 台の機器間の位置関係は自由になる．後述するようなプロトコルにより，近接モードによって安全に鍵交換を行うので，以後の通常モードのワイヤレス通信の秘匿性も守られる．

この方式では近接の通信を実現するための付加的なハードウェア・センサーが不要になるので，普及が予測されている無線 LAN 機能つきの携帯デバイスで，特殊なハードウェアの装備を前提とせずに利用できる可能性を持っている．

図 2. 近接モードの導入によるワイヤレス接続設定

本研究で利用している機器構成では，ワイヤレス通信には 802.11b を用いている．ほとんどの 802.11 用の無線 LAN 用チップセットは，送信出力を制限すること，受信パケットごとに信号強度を計測する機能を備えている．信号強度は，原理的には距離の二乗に反比例するが，機器の方向，間にある遮蔽物，マルチパス等の影響を受ける．したがって二つの機器がある程度以上はなれてしまうと，信号強度情報のみから両者の距離を推定することは困難である．

しかし，両者が極めて近い位置関係にある（たとえば 30cm 程度以内）場合は，信号強度が著しく増加するので，閾値との比較によって近接関係を判定することができる．

なお，本論文の実現は 802.11b の通信プロトコル・ワイヤレスチップセットに基づいているが，他の 802.11a/g, Bluetooth 等の無線通信技術への拡張も可能である．

3　システム・アーキテクチャー

本研究で対象とするワイヤレス通信は，大きく 2 種類に分類できる．ひとつめはアドホック・モードで，機器間が直接通信する形態である．もうひとつはインフラストラクチャモードで，機器は設置されているアクセスポイントを介して通信する．

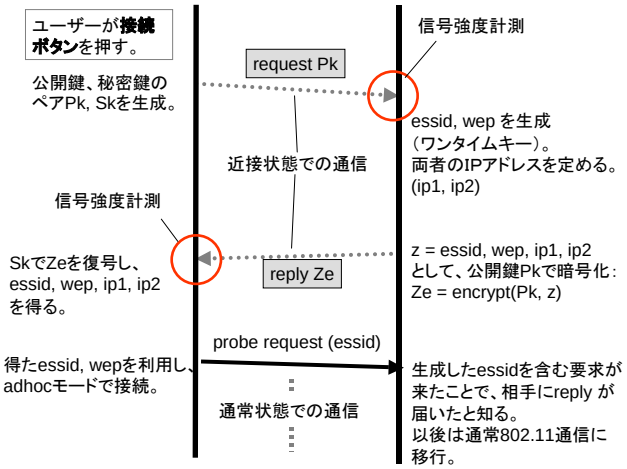

図 3. アドホック・モード接続時のプロトコル

3.1　アドホック・モード接続

アドホックモードでは，2 台の機器が通信を開始する前に，両者の相互認証，使用する秘密鍵の共有を行う必要がある．具体的なプロトコルを図 3 に示す．この図の破線で示されている通信は，機器を近接させた状態で送受信する．図に示されているように，最初にどちらかから接続要求のパケットを出す（事前に役割を決める必要はない）．接続要求パケットはブロードキャストであり，送信先を指定していない．接続要求受付側は，接続要求パケットの信号強度が一定以上のときのみ自分宛て要求だと判断し，返答を返す．この返答パケットも，近接状態で送られているかどうかを確認するために，接続要求側で信号強度を測定する．したがって，接続要求パケットを受信した第三者が，通信相手になりすまそうとしても，第三者が近傍関係にない場合には，接続要求側で拒否することができる．互いに相手から受信したパケットの信号強度をチェックすることで近接モードであるかどうかを判定している．

また，返答に WEP キーなどの秘密情報が含まれるので，受信した公開鍵で暗号化して傍受から守っている．今回の実現では，セッションごとに WEP キーを新規生成し，それを返答に含めている．

このようにして，2 台の機器をアドホック無線により接続することができる．利用者側からみると，必要な操作は単に 2 台の機器を接近させて，接続開始（たとえばボタンを押す）を指示するだけである．事前に相手の機器 ID やアドレスを知る必要がなく，WEP キーなどを手入力する必要がない．また，鍵情報を接続セッションごとに新規生成するので安全に通信を行うことができる．

なお，本プロトコルでは簡単のために「近接関係にあれば無条件でアクセスを許す」という方針になっているが，従来型の認証と組み合わせて「権利を持っている機器が接近したら許す」というポリシーにすることももちろん可能である．また，今回の実現では WEP キーを用いているが，802.1x 認証や WPA に拡張することも容易であろう．

3.2　インフラストラクチャ・モード接続

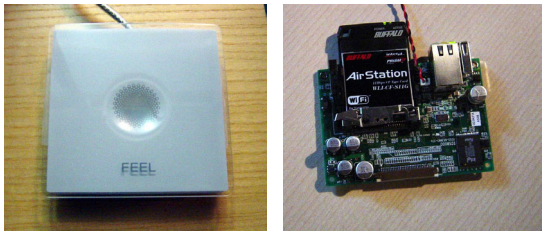

図 4. ダミーポイント試作例

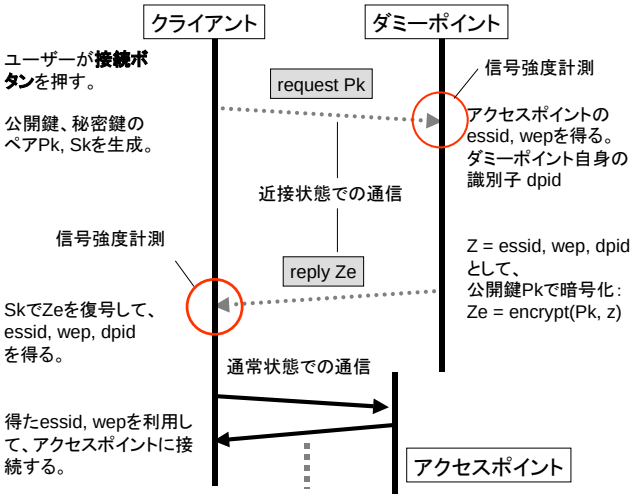

図 5. ダミーポイントを利用したインフラストラクチャモード接続時のプロトコル

一方，インフラストラクチャモードでは，各機

器はアクセスポイントへの接続と，機器間のサービスの接続の２種類を考慮する必要がある．前者は，機器がアクセスポイントが管轄するワイヤレス環境への通信を設定するための操作であり，後者は（すでにこのようなフェーズを経て通信が可能になっている）機器の間での特定のセッションを開始するための操作である．たとえば，携帯機器に格納されている画像ファイルを，自分の目の前にあるプリンタで印刷する，などの場合がこれに相当する.（この場合，携帯機器とプリンタはアクセスポイント経由で通信しているものとする）.

3.3　ダミーポイント

前者の接続に対しては，アドホック・モードのときと同様に，携帯機器をアクセスポイントに近接させて接続要求を行う方法がまず考えられる．たとえばアクセスポイントがテーブルやカウンターの上に置いてある環境ではこの方式を使うことができる．しかし，実際にはアクセスポイントは天井付近など，機器から物理的にアクセスしにくい場所に設置される場合が多い．

そこで,「ダミーポイント」という概念を導入する．ダミーポイントは，近接モードでの返答のみに特化したアクセスポイントで，実際のワイヤレス通信は担当しない．ダミーポイントは，アクセスポイントにワイヤレス接続するために必要な情報（ESSID や WEP キー）の配信に利用する．ダミーポイントの数はアクセスポイントとは無関係に複数置くことも可能である．ダミーポイント内に ESSID や WEP キーなどの情報を格納する適当な手段（たとえば USB メモリースティックなど）があれば，ダミーポイント自体がネットワークに接続されている必要は必ずしもない．

ダミーポイントの試作例を図 4 に示す．この例では，シングルボード Linux(L-Card) と無線 LAN カードによって構成している．ダミーポイントを利用した場合の実際のプロトコルを図 5 に示す.

ダミーポイントは，利用者がアクセスしやすい場所，たとえばテーブルの上などに設置しておくことが考えられる．ワイヤレス環境に接続したい利用者は，まず機器をダミーポイントの近くに置いて「接続ボタン」を押せばよい．これは,「ダミーポイントに物理的に接近できる」ということを暗黙のアクセス権として利用していることになる.

また，ダミーポイントとしてスティックのように手持ち型の装置を想定することも可能である (図 6). たとえば屋外のホットスポット等で，スティックを近づけて機器の接続開始を指示することができる.

ダミーポイントによるアクセス制御

ダミーポイントは同じアクセスポイント配下のワイヤレス環境に複数個設置できる．また，ダミーポイントからの返答に，ダミーポイント自体の識別情報や，コンテキスト情報（位置・ダミーポイントが対応している他のネットワーク機器）を含めることが可能である．この性質を利用して，ダミーポイントを実空間でのワイヤレス環境への仮想的な入り口として利用することが可能になる.

図 6. 手持ち型ダミーポイントの例

たとえば，プリンタ横に設置してあるダミーポイントに携帯機器を近づけた場合，携帯機器の標準出力先が，対応するプリンタに自動設定するようなアプリケーションが構築可能である．ダミーポイントの粒度とデバイスの粒度は利用目的によって自由に設定できる．たとえば，ダミーポイントに携帯機器を近づけると，その部屋に置かれている機器にアクセス可能になる，などの設定が可能である．この場合部屋に設置された機器数は限られているので，その中からの選択手法としてメニュー選択などを使うことが考えられる.

これに類似した機能は，非接触タグ・リーダーの組み合わせを利用しても実現できるが，ダミーポイントを利用した場合，携帯機器側に何ら特別な付加ハードウェア・センサを準備する必要がないので，ワイヤレス機能を装備した任意の携帯機器で利用できる点が特長だといえる.

図 7. ２台の機器間でアドホック接続を設定

3.4 システム実現

以上のプロトコルを実現するためには，通常のワイヤレス接続のプロトコルに先立って，パケットごとに信号強度が判定できる，ブロードキャストパケットの送受信が必要である．802.11 では通常のデータ通信を担当するデータフレーム以外に，機器の存在を確認するプローブ要求，ビーコンなどのマネージメントフレームがある．通常はマネージメントフレームの処理はデバイスドライバが担当し，ユーザーレベルプログラムから直接送受することができない．

今回の実装では，Linux のワイヤレス LAN デバイスドライバ [3] に改造を施して，ユーザレベルプログラムからのマネージメントフレームの送受信を可能にし，その上に上記のプロトコルを構築している．近傍での通信が完了すると，通常のワイヤレス通信が利用可能になるので，既存のアプリケーションソフトウェアをそのまま利用することができる．

4 アプリケーション例

4.1 アドホック環境でのファイル交換

図 7 は 2 台の機器間でのファイル交換を行っている例である．交換に先立ち，2 台の機器を接近させて接続モードに入る．接続が確立されてからは近接関係を維持する必要はない．ファイル交換は，接続フェーズで互いに相手の IP アドレスを交換しているので，利用者が相手の機器のアドレスを指定する必要はない．両者の画面を共有して，ファイル実体の送信に先立ち，送信すべきファイルのサムネイルを指定しあうようなアプリケーションを構築することも可能である．USB メモリーを経由してファイルを渡す場合と比較して，双方向で，よりインタラクティブな情報交換が可能である．

4.2 対戦型ゲームの環境設定

図 8. ワイヤレス・対戦型ゲームへの適用例．シングルユーザ・モードから機器を接近させて動的に対戦相手と接続することも可能である．

対戦型ゲームをワイヤレス携帯機器に適用した例を図 8 に示す．図ではテトリスが動作しているが，2 台の機器を接近させて「接続」ボタンを押すと，ゲームモードが動的に対戦型テトリスに切り替わる．

4.3 公共ディスプレイからの情報取得・アップロード

図 9. 公共ディスプレイへの情報の登録. 写真ファイル等を，ディスプレイ付近に設置されたダミーポイントに携帯機器を接近させて送信する．

図 9 はオフィス内に設置された公共ディスプレイである．利用者は，携帯機器を公共ディスプレイ下に設置してあるダミーポイントに接近させることで，通信環境が設定され，ファイルを自由にアップロードすることができる．このようにして，通りすがりに情報を公開したり取得したりする電子掲示板が構成できる．

同様な方式で，会議室のプレゼンテーションスクリーンにワイヤレス経由で画像を投影するための設定などを行うことができる．

その他，画面やインタラクションの手段を持たない装置，たとえばファイルサーバーや組み込みセンサーに対応させてダミーポイントを設置すれば，機器のメインテナンスに応用することができる．ワイヤレス機能をもつ PDA やノート PC などを接近させて，サーバーの内容を調べたり変更したりするための Web 画面を呼び出すことができる．

5 議論

5.1 関連研究

情報の接続関係を直接操作インタフェースで制御しようという発想は，Pick-and-Drop[4] や MediaBlock[8] などで提案された．両者とも中間的なオブジェクト（ペンやブロック）を利用しているが，我々のアプローチは機器間のネットワーク接続を制御している．

Swindells らは PDA に赤外線発信装置を，各機器に赤外線受光器を添付して機器間のアドホックな接続制御に用いている [7]．機器特定に直接的な関

係を持ち込むという点で近いアプローチであるが，デバイス間での安全な接続を考慮していない．

5.2 通信の安全性

本方式は，通信を開始する際に，双方が相手からのパケットの信号強度を確認し，それが一定値以上でないと受け付けないようにしている．このことで，近接関係にない機器が通信相手に「なりすます」ことを防いでいる．

ただし，信号強度は送信出力に依存するので，たとえば仮に 10 倍の距離にある機器から 100 倍の送信出力でパケットを送ってきた場合，それを近傍からの要求だとみなしてしまう危険性がある．現実的には，このように特別なハードウェアを必要とする不正利用はソフトウェアだけのセキュリティーホールと比較して起こりにくいといえるが，考えられる対処法としては，以下が挙げられる．

- 近接送信に対する返信の送信出力を下げる．近接関係にある機器では受信できるが，遠方の機器では受信できず，通信が成立しない．
- 複数のダミーポイントからの情報を統合する．たとえば，2 台のダミーポイントがあれば，物理的に近接している場合は特定の 1 台が受信する信号強度だけが突出して大きくなるが，遠隔地から高出力で送信してくる場合にはその差が顕著になりにくい．

一方，2 者の間に入って，互いに反対側の通信相手に「なりすます」(man-in-the-middle attack) は，ワイヤレス通信という性質上，送信されたパケットを完全にインターセプトできないかぎり本質的に困難である．

また，近接関係の通信であっても，ワイヤレス通信の到達範囲内にいる第三者が通信内容を傍受することは可能なので，セッションキーなどの秘密情報を直接送受することは危険である．本提案の方式では相手が送ってきた公開鍵によって暗号化して秘密情報を返すので，通信傍受による被害は公開鍵暗号の強度によって守られている．

5.3 近接証明：近接関係だった事実を認証に利用

ネットワーク操作の他の可能性として，上記のようなプロトコルを用いて，機器 A と B が過去のある時点で近接関係にあったことを証明する記述（証明書）を発行することが可能である．これを利用して，次の機会に遠隔地から機器にアクセスする場合でも，過去近接関係にあった機器を別扱いすることができる．

たとえば，家庭にあるホームサーバーに携帯電話を近接関係にしてネットワークを構築し，ホームサーバーにあるコンテンツ名と近接関係を組みにして証明書を発行する．以後，外部からホームサーバーのコンテンツにアクセスする場合には，携帯機器に格納された証明書の所有をホームサーバー側から問い合わせることで認証が可能である．別の可能性としては，会議室などで同席した人どうしを近接関係の証拠として記録しておき，以後その証拠を持っている人のみが参照できる情報を発信することができる．

6 結論

本論文では，ワイヤレス機器の接続関係を，利用者が簡単な操作で制御できる方式・プロトコルを提案し，試作システムを構築した．具体的には，ワイヤレス接続を確立するフェーズで，受信パケットの信号強度を計測することで，2 台の機器が近接関係にあることを判定する．また，ワイヤレス通信で用いるための鍵情報を，安全な方法で共有するプロトコルを提案している．

本方式は，無線 LAN 機能をもったデジタル機器において，特別な付加ハードウェア・センサーを必要とすることなく利用できるので，すでに普及が開始している携帯型ワイヤレス機器のユーザインタフェースとして広く利用することが可能である．たとえば，街角で即座にアドホックネットワークを構築してファイル交換や対戦型ゲームを楽しむ，といった利用に適用できる．

参考文献

[1] Yuji Ayatsuka, Michimune Kohno, and Jun Rekimoto. Shownpass: an access control with a displayed password. In Proceedings of Interaction 2003, IPSJ Symposium Series Vol.2003, No.7, pp. 155–162. IPSJ, IPSJ, February 2003.

[2] Michimune Kohno and Jun Rekimoto. New generation of ip-phone enabled mobile devices. In 4th International Symposium on Human Computer Interaction with Mobile Devices (MobileHCI2002), pp. 319–323, 2002.

[3] Jouni Malinen. Host ap driver for intersil prism2/2.5/3. http://hostap.epitest.fi/.

[4] Jun Rekimoto. Pick-and-Drop: A Direct Manipulation Technique for Multiple Computer Environments. In Proceedings of UIST'97, pp. 31–39, October 1997.

[5] Jun Rekimoto. Synctap: An interaction technique for mobile networking. In Proc. of MOBILE HCI 2003, 2003.

[6] Jun Rekimoto, Yuji Ayatsuka, Michimune Kohno, and Haruo Oba. Proximal Interactions : A direct manipulation technique for wireless networking. In Proc. of INTERACT 2003, 2003.

[7] Colin Swindells, Kori M. Inkpen, John C. Dill, and Melanie Tory. That one there! pointing to establish device identity. In Symposium on User Interface Software and Technology (UIST'02), pp. 151–160, 2002.

[8] Brygg Ullmer, Hiroshi Ishii, and Dylan Glas. mediaBlocks: Physical containers, transports, and controls for online media. In SIGGRAPH'98 Proceedings, pp. 379–386, 1998.