IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 05-11
www.iosrjournals.org

An Enhanced Secure Protocol For Spontaneous Wireless Ad-Hoc Networks

[1]Nimisha paulose, [2]Sindhu M P
[1]*Computer Science and Engineering Sree Narayana Gurukulam College of engineering Ernakulam, India , nimishapaulose24@gmail.com*
[2]*Associate Professor Computer Science and Engineering Sree Narayana Gurukulam College of engineering Ernakulam, India, sindhuvino@gmail.com*

Abstract: *The main aspect of wireless ad hoc network communication is using of security so this paper proposing a secure protocol for spontaneous wireless ad hoc network. This protocol offers network creation, and management of communication within a spontaneous network. We introduce the notion of a spontaneous wireless network, created when a number of peoples come together for certain period of time, for collaborative activities. This protocol includes all functions need to operate without any external supports. Protocol runs on the basis of trust between the collaborating peoples in the network. It uses a hybrid symmetric and asymmetric key encryption schemes for user authentication. This paper describes a secure protocol with an intrusion detection mechanism for spontaneous wireless ad hoc network*

I. Introduction

Spontaneous ad hoc networks are formed by a set of mobile nods placed in a close location that communicate with each other, share resources, services in a limited space by following human interactions patterns [1,2]. Spontaneous network is a special case of mobile ad hoc network. It can be wired or wireless, but in this paper we considered only wireless network.

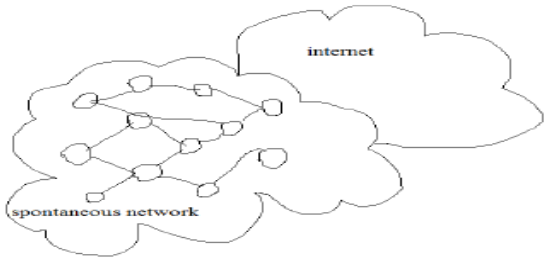

Figure 1: Network Model

Spontaneous wireless ad hoc network require a well defined, efficient and user-friendly security mechanism. Main tasks can be identification of user, their authorization and assignment of address, authentication and trust. In this network nodes establish routing among themselves dynamically to their own as shown in figure 2. A certificate authority (C A) is used by wireless ad hoc network to manage authentication of node and trust [3]. In wireless ad hoc network C A is used to authenticate the users. Network allows user to join into the network. Hence the new user is trusted by certification authority [4, 5]. A major problem in mobile ad hoc network is management and dissemination of information. Since the mobile devices are restricted in their resources, a complete copying of information will not be possible.

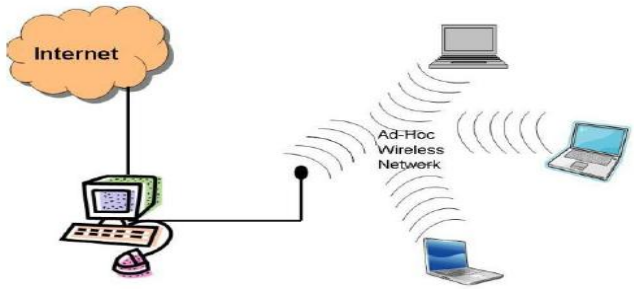

Figure 2: Spontaneous network model

In this type of network, it is not preplanned hosts are not preconfigured. There will be no server and the users are not experts. There are main features of spontaneous network. Cooperation among the nodes and quality of service for all shared network services should be provided [6]. Security should be based on confidentiality, cooperation and privacy. All nodes may not be able to execute the routing or security protocols. Dynamic network with flexible member and group signature are difficult to manage [7]. For reliable communication in the mobile ad hoc networks, it requires key exchange mechanism for node authorization and user authentication. Several security methods such as pre distribution key algorithm [8] symmetric and asymmetric algorithm, intermediate node- based method [9] and hybrid methods [10].

II. Related Works

Ad hoc networks operate independent of an access point infrastructure, whereas still different administrative services. The methods used earlier enable the user to get service without any requirement of any external infrastructure. Some nodes may not be able to run the security and routing protocols. So it is necessary to use of adaptive routing and security for any types of devices and scenarios. In [11] latvakski et al. explained a communication architecture concept for spontaneous systems for integrating application-level spontaneous group communication and ad hoc networking together. Gallo et al. [12] pursued two targets in spontaneous networks: to maximize responsiveness given some constraints on the energy cost and to minimize the energy cost given certain requirements on the responsiveness.

In [13] untz et al. proposed an efficient and light weight protocol for inter connection suitable for spontaneous edge networks. They designed and implemented a prototype of an interconnection protocol called Lilith for spontaneous edge networks. It uses MPLS and allows different communication paths on a per flow basis and back-up paths. It makes available information on destination reach ability. In [14] feeney et al. proposed Spontnet a protocol implementation of simple ad hoc network configuration based on spontaneous networks. It allows user to distribute a group session key without previous shared context and to establish shared namespace. A simple web server and a shared white board are providing as examples of collaborative applications. They use IPSec protocol which is used for Virtual Private Network (VPN) applied through internet.

Danzeisen et al. [15] apply WEP, the regular security mechanism used in Wireless LANs, available by default in the IEEE 802.11 wireless protocol. Other proposals that did not discuss security aspects it could also apply default solution. It is available to us, we did not use it because WEP is vulnerable to hacking attacks and better solutions, and WPA2 can be considered instead.

Ba¨ckstro¨m and Nadjm-Tehrani [16] developed first real spontaneous network. It offers many services dynamically using the Jini technology and they explained the architecture of the contact service and the implementation. Czerwinski et al. [17] introduced an architecture and implementation of a secure Service Discovery Service (SDS). Clients as well as Service providers use SDS to create complex queries for locating these services and to advertise complex descriptions of existing running services respectively. It facilitates the network enabled devices to discover available. The core component of secure service discovery service is security and, communications and both encrypted. Certificate authority signs certificates, whose public key is known to everyone. The components include clients which want to discover services that are running in the network and servers respond to client queries. To control the access to service information, it uses a hybrid access control list.

Zhu et al. [18] developed a light-weight secure protocol for ad hoc networks. Most of the routing protocols for ad hoc networks do not apply network access control and it causes the networks susceptible to resource consumption attacks where a malicious node injects erroneous routing updates into the network with the goal of paralyzing the network. In order to prevent such attacks, it is necessary that a node joining ad hoc network employs some authentication mechanisms. Spontaneous networks are also special case of human centric networks [19]. Cornelius et al. implemented and evaluated Anony Sense, a general-purpose framework for anonymous opportunistic tasking and reporting. It allows applications to query and receive context through an expressive task language.

Rekimoto presented a concept of Sync Tap on user operation in [20], also described user interface Sync Tap technique. It can be used in spontaneous network for establishing network connection between digital divices. This method can deal with multiple overlapping connection requests by detecting “collision” situations. It can also ensure secure network communication by exchanging public key information upon establishing a connection. Shared session key is created by piggybacking Diffie-Hellman public keys (generated by each device) on multicast packets. These public keys are used to calculate a shared secret session key in encrypted

communication. In this case, the authors do not propose any secure protocol but they have just added an existing security mechanism in their authentication. It is similar to the one used by us when a new node joins our network, but we have added other security mechanisms to create a complete secure protocol.

III. Spontaneous Networks

A. Overview

The spontaneous network can be wired or wireless. Spontaneous network share resources, services during a period of time and in a limited space [21]. The main goal of spontaneous network is collaboration of devices and services at one place allowing user to have instant service without external support. This network is implemented basically in mobile phone, PDA, laptops with limited memory space and energy. Users in the spontaneous network are not need to identify all participants are administratively configure their computer in advance, while still connected to their house networks. A spontaneous network reflects intentional interactions among users who have chosen to collaborate for some purpose. It is this intentionality that can be leveraged in order to create on ordered method for starting the network configuration. Spontaneous network should complete the following steps to be created [22].

B. Procedure for joining the network

This step enables the devices to join to the network and communicate in between the devices in the same network. For this purpose, the system uses user an Identity Card (IDC) and certificate. The IDC contains private and public components. The public component contains a Logical Identity (LID). Logical identity is unique for each user and it is used to identify it. It may include information such as name and email id or other types of user identification. This method has been used in other systems like vehicular ad hoc network [23]. It also contain public key (Ki) of the user, and the user signature. This user signature is created using the Secure Hash Algorithm (SHA-1) [24] on previous data to obtain the data summary. Then this summary is signed with user's private key. The certificate Cij of the user i consist of a valid IDC, signed by a user j that given its validity. No central authority is used to validate IDC. When node A wants to communicate with another node B and it requests it from its trusted nodes. After obtaining this certificate the system will validate the data; if correct then it will accepts node as a valid node. All nodes can be either clients or servers, and can request or serve requests for information or authentication from other nodes.

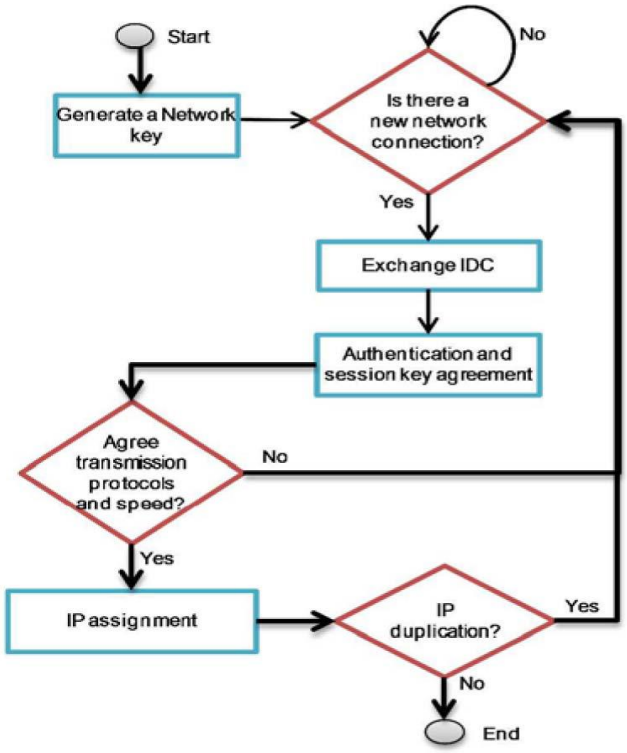

Figure 3: Procedure for joining a new node

The first node will create the spontaneous network and generate a random session key, which is exchanged with the new node after authentication. Fig 1 shows the procedure for a node to joining the network. When a node B wants to connect to a network it should have to chose a node within its communication range to authenticate with (e.g. node A). Then A will send its public key to B. Then B will send its IDC signed with A's public key. Next A will validates the received data verifies the hash of the message in order to check that the data is modified or not. The node A establishes a trust level of B by looking physically. Finally node A will send its IDC to B. This data will be signed with A's public key. Then B validates the data which is received by integrity verification and authentication. If in the first step A does not replay to the node, then B should have to choose another node within the communication range. After the authentication phase B can access data, services within the network. For security purpose it uses symmetric key encryption scheme which is Advanced Encryption Standard (AES) [25]. It offers high security because its design structure removes sub key symmetry.

C. Service discovey

The user in a network can ask for other devices in order to know available services. The services can be data transfer, print services, etc. the node can request for any node with a service and get access the service for the particular time period [26]. The service provided by B will be available only thenode B exixts in the network. The service disappered when B leaves the network.

D. Trust chain management

There are two level of trust in the system, either trust or does not trust. Node can either trust or does not trust the new node. The trust relationship can be asymmetric. If node A did not establish trust level with node B directly, it can be trusted through trust chain e.g. if A trust C and C trust B, then A may trust B.

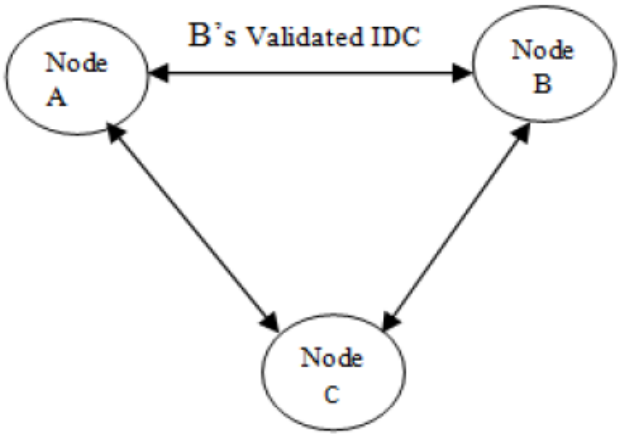

Figure 4: Trust chain model

It can also stop trusting if it discovers that previous trust chain does not exist anymore.

III. Protocol Working

The network is created using the information provided by user each node is identified by an IP address. The network is built using IEEE 820.11b/g technology. This technology has high data rates to share resources.

E. Joining new node

This protocol relies on a sub layer protocol which can be Bluetooth [27] or zigbee. Once the registration phase process of the user in the devices has been done, then it must determine whether to create a new network or participate in an existing network. If the user decides to create a new network it begins the procedure shown in fig 5.

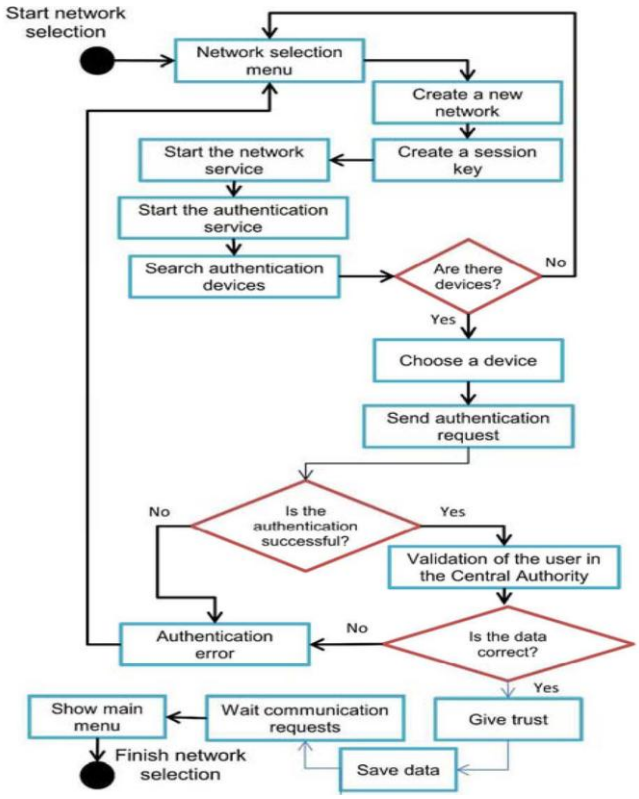

Figure 5: Procedure for new network creation

When the node finishes its registration phase its session key will be generated this session key is a random number. Then its session key will be send to the validating node. Then it can access the services. After accessing the service this node can leave the network. Intrusion detection system is used in this network to detect the node which can be attackers. These nodes can be added to the real network nodes by the authorities. The nodes can leave the network without any restrictions. When devices leave the network its service which is provided by them also be removed.

F. Intrusion detection

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users).

In this spontaneous network Intrusion detection is used here as a security mechanism to protect the network from unauthorized accesses. A table shows the real network nodes, available nodes and attacker nodes. The attacker nodes are not actually attackers; there is a possible chance of attack from these nodes. The newly created devices are actually placed in this attackers list and the authorities can add these nodes to the real network node if they are trustable.

G. Protocol operation

When a device wants to connect to a network then it should register its personal details in the system. User should have a valid email id for registering to the spontaneous network. After authentication the devices can perform any services like data store, data transfer, and print services etc. An authenticated user can perform these activities in the network.

- Display the nodes.
- Update the information.
- Process an authentication request: The node authenticates a requesting node by validating the received information, user authentication, and verifying the no duplication of the LID data and the proposed IP.

- Reply to an information request: the requested information will be sent directly to the requesting node or routed if the node is not on the communication range.
- Send data to one node: It can be sent symmetrically or asymmetrically encrypted.
- Leave the network

IV. Implementation

The security in spontaneous network depends on the symmetric and asymmetric key encryption schemes that are used. Session key generated as a random number and, it is used to encrypt the secret messages among trust nodes. The algorithm used for the symmetric encryption scheme is Advanced Encryption Standard (AES) whereas for asymmetric key scheme is Rivest, Shamir and Adleman (RSA). The process of Session key and authentication of node are distributed using asymmetric key encryption algorithm. Only user can determine whether it has to build a network or to join in an existing one once validation is completed. The node that wants to join a spontaneous network begins the procedure by sending a Discovery request packet to the other nodes in the same network. The packet which is sending contains the LID of the sending node. The receiving packet contains the LID and IP address of the nearest node in the network. The data received is used to study the chosen device to authenticate or not. Authentication request and reply packets are used for device authentication.

H. Implementation results

- Any new node can register into a network with specifying its own service that provides and it will be added to the network based on the trust.
- Newly created node should be mutually authenticated to the nearest node in the network.
- The newly created node can generate the public and private keys.
- The nodes are placed under the services that are commonly provided like data store, data transfer and print service.
- Nodes in the network can connect to the network through any of its nearest node.
- After mutual authentication this node can only communicate to the nodes in the network.
- Then it should create the session ID for a particular time of communication and send its session ID to the authenticated node.
- The node can access the services from any other nodes in the same network, so it doesn't want to be authenticated at all time of communications.

V. Conclusion

In this paper we had designed a secure protocol for spontaneous wireless ad hoc network; it permits secure communication among trust nodes. The spontaneous networks are developed to accomplish a collaboration of tasks on a limited space and time. A new user had its own provision that to join to a network or create a new network. The devices in the network can perform many services like data transfer, print service etc. the node can leave the network whenever it wants, or when it completes the tasks. When the devices leave the network then the service provided by that device will be automatically removed.

Intrusion detection is implemented as a chance of intrusion can occur in the network. After checking the hash value generated then it will assigned as attacker node. Basically all new nodes added to the network are considered as attacker node, the administrator can add the node into the real network data base then it will treat as real nodes. When a node is add to a real node then it will not be an attacker node.

References

[1] L.M. Feeney, B. Ahlgren, and A. Westerlund, "Spontaneous Networking: An Application-Oriented Approach to Ad-hoc Networking," IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2001.
[2] J. Lloret, L. Shu, R. Lacuesta, and M. Chen, "User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless Networks," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/ 2, pp. 1-8, 2012.
[3] Xiao Y. Rayi V.K., Sun B., Du X., Hu F. and Galloway M. (Sept.2007)"A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341.
[4] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept.2007.
[5] V. Kumar and M.L. Das, "Securing Wireless Sensor Networks With Public Key Techniques," Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.
[6] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. WirelessComm. and Networking, vol. 2010, article 18, 2010.

[7] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.
[8] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks," Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.
[9] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.
[10] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.
[11] J. Latvakoski, D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems," IEEE Wireless Comm., vol. 11, no. 3, pp. 36-42, June 2004.
[12] S. Gallo, L. Galluccio, G. Morabito, and S. Palazzo, "Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks," Proc. Seventh ACM Int'l Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Oct. 2004.
[13] V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '04), Aug. 2004.
[14] L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels,"Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks," Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.
[15] M. Danzeisen, T. Braun, S. Winiker, D. Rodellar, "Implementation of a Cellular Framework for Spontaneous Network Establishment," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.
[16] J. Ba¨ckstro¨m and S. Nadjm-Tehrani, "Design of a Contact Service in a Jini-Based Spontaneous Network," Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., Aug. 2001.
[17] S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H., "An Architecture for a Secure Service Discovery Service," Proc. ACM/IEEE MobiCom, Aug. 1999.
[18] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hop by-Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., pp. 567-585, vol. 4, no. 5, Sept. 2006.
[19] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-Aware People-Centric Sensing," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08), pp. 17-20, June 2008.
[20] J. Rekimoto, "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134, May 2004.
[21] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "*Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems*," Ad hoc and Sensor Wireless Networks, vol. 14, nos. 1/2,pp. 107-132,2012.
[22] L.M. Feeney, B. Ahlgren, and A. Westerlund, "Spontaneous Networking: An Application-Oriented Approach to Ad-hoc Networking," IEEE Comm. Magazine, vol. 39, no. 6.
[23] J. Sun, C. Zhang, Y. Zhang, and Y. (Michael) Fang, "An Identity- Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.
[24] FIPS 180-1 - Secure Hash Standard, SHA-1, "National Institute of Standards and Technology," http://www.itl.nist.gov/fipspubs/ fip180-1.htm, Feb. 27, 2012.
[25] S. Landau, "Communications Security for the Twenty-First Century: The Advanced Encryption Standard," Notices of the Am. Math. Soc., vol. 47, no. 4, pp 450-459, Apr. 2000.
[26] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Adhoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.
[27] R. Lacuesta and L. Herrero, "A Good Use of Bluetooth, A Good Use of Bluetooth," Proc. Int'l Workshop Advanced Web Eng. for e- Business (AWEEB '04), Mar. 21, 2004.