A Role-based Probabilistic Routing Protocol for Bluetooth Ad Hoc Networks

Abstract:

As mobility of personal electronic devices becomes more the rule than the exception, ad hoc networking is becoming increasingly important. By definition, ad hoc networking does not rely upon an established communication infrastructure, but it can be used either to augment currently existing communication infrastructure or to operate in places where the communication infrastructure is inoperable (due to natural disaster, terrorist attack, or simply extreme user traffic congestion) or nonexistent (a scenario that can arise in remote rural areas). Two common technologies for creating ad hoc networks are Wi-Fi (IEEE 802.11) and Bluetooth (IEEE 802.15), the latter of which we will be using for our research. The scenario that we will be using for our investigation will revolve around the idea of disseminating alert messages in emergency situations in high-population areas (e.g. a professional or collegiate sports venue on game day).

In ad hoc networking, particularly those established via Bluetooth, the primary issues involved include routing, security, and trust. Generating solutions for these issues becomes even more important when the technology is meant to aid those who are in emergency situations. In terms of routing, there have been multiple proposals for developing an efficient protocol. Some examples of routing protocols include:

- Routing Vector Method (RVM): Uses packet forwarding to construct a path from source to destination. Upon receipt of the route "search" packet, the destination node sends a reply along the established route.
- Bluetooth Master-Managed Routing (BMR): Master nodes within the ad hoc network use the links of surrounding nodes to build a table that contains routing information.
- Location Aware Mobility-based Routing Protocol (LAMP): Combines some of the features of RVM and BMR.

A common feature among each of these protocols is the idea of establishing a route in the network prior to sending any non-control packets. Depending on the complexity of the network, this could result in a lot of overhead and there is no guarantee that the delivery path will be valid when the source attempts to deliver the non-control packet(s).

Security and trust are often paired with the issue of routing since users want to be sure that the intermediate nodes they use to relay messages are trustworthy. Projects such as SHIELD and iTrust sought to develop methods for establishing trust between devices by using trace analysis of encounters between mobile nodes. The difficult part about using trace analysis is that developing a network of trust using trace analysis can take a longer period of time.

Our proposed routing protocol will attempt to address the issues of both routing and security/trust through the use of roles. Each node in the ad hoc network will be labeled as either a Civilian node or an Authoritative node. Furthermore, each node in the network will have a point value that corresponds to the number of neighbors that node has and the role of each of those neighbors. Nodes with a high number of neighbors will have higher scores and those nodes whose neighbors are of the target role (i.e. neighbors who are labeled as Authoritative) will be given even higher scores. When a Civilian node generates a message that is destined for

an Authoritative node, the source node forwards its message to its neighbor that has the highest score. This process repeats from one node to the next until the packet reaches an Authoritative node (note that packets in this protocol are aimed at any node whose role is "Authoritative," not one particular node). The idea behind this approach is that the intermediate nodes with higher scores are either near nodes that have the target role or near many other nodes that may in turn be near nodes with the target role. Although this probabilistic approach does not guarantee delivery of the packet, it reduces the amount of overhead by eliminating the control packets that are often used by other routing protocols for route discovery.

To tackle the issue of security, the roles will be used in determining the encryption and decryption of messages. When a Civilian node generates a message, the message will be encrypted in such a way that it can only be read by using a key that is available only to Authoritative nodes. For all other Civilian nodes that act as intermediate nodes in the packet forwarding process, those nodes will not have the proper key and will thus not be able to read the message. The process of forwarding the message to other nodes will be handled in the background without requiring user interaction. As a result of these two security measures, if a malicious user receives the packet, not only will they not be able to read the message, but also their node will still forward the packet to another node in the network.

References:

[1]-Dunne, Kevin, Elaine Roche, David O'Loghlin, and Ewis Rhatigan. "Bluetooth for Ad-Hoc Networking." *NTRG: Networks & Telecommunications Research Group*. Networks And Telecommunications Research Group (NTRG), Trinity College Dublin, Ireland, 25 Feb. 2005. Web. 29 Feb. 2012. <http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group3/index.html>.

[2]-Whitelock, Ron. "Bluetooth! A New Technology for Transportation?" *IMSA Journal* (2011): 20. Print.

[3]-Sheng-Wen Chang; Sahoo, P.K.; Li-Ling Hung; Chih-Yung Chang; , "A location-and-mobility aware routing protocol for Bluetooth radio networks," *Pervasive Computing (JCPC), 2009 Joint Conferences on* , vol., no., pp.137-142, 3-5 Dec. 2009
doi: 10.1109/JCPC.2009.5420199
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5420199&isnumber=5420061

[4]-Bhagwat, P.; Segall, A.; , "A routing vector method (RVM) for routing in Bluetooth scatternets ," *Mobile Multimedia Communications, 1999. (MoMuC '99) 1999 IEEE International Workshop on* , vol., no., pp.375-379, 1999
doi: 10.1109/MOMUC.1999.819514
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=819514&isnumber=17761

[5] Song, O.; Chaegwon, L.; Chong-Ho, C.; , "Mobility Management in Bluetooth ad hoc networks,"
Samsung Electronics, 2004. The 14th Joint Conference on Communications & Information, JCCI 2004.
URL: http://csl.snu.ac.kr/publication/paper/JCCI_BMR_final.pdf

[6] Scarfone, K.; Padgette, J.; , "Guide to Bluetooth Security," *National Institute of Standards and Technology (NIST), Special Publication 800-121*, pp. 3-2,
URL: http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf

[7] Kumar, U.; Helmy, A.; , "iTrust", URL: http://128.227.176.22:8182/iTrust.html

[8] G. Thakur, M. Sharma, A. Helmy, "*SHIELD*: Social sensing and Help In Emergency using mobiLe Devices", *IEEE GlobeCom (Global Communications Conference)*, Dec 2010.