

# ICITST 2006

International Conference for Internet Technology and Secured Transactions  
September 11–13, 2006, London, United Kingdom



## Ad-hoc Messaging Network in a Mobile Environment

Christoph Fuchß

Virtimo webbased applications, Germany

Stefan Stieglitz

University of Potsdam, Germany

Oliver Hillmann

Eyze.org, Germany

**Abstract:** In recent years a growing number of mobile services have been offered. Most of these data based applications follow the mechanisms of 'fixed internet' even to support mobile networks. This approach reflects the attempt to transfer internet applications to mobile networks under conditions of stability, speed, and flexibility. Furthermore the structure and characteristics of the network should be transparent for applications. This method causes problems in routing algorithms for MANETs. This contribution follows a new approach and focuses on 'messages' as the central point of interest. The paper shows how to provide message-centric mechanisms of ad-hoc networking in local environments by simple means and protocols like store-and-forward routing and points out applications that use these network specifics. Furthermore the concept of Ad-hoc Messaging Network (AMNET) is introduced which allows to implement a wide range of mobile applications in a more efficient way than merely relying on MANETs. By using the specific characteristics of mobile networks and making them available for applications, significant advantages can be gained by adopting the concept of AMNETs.

**Keywords:** Mobile, ad-hoc networks, e-payment, MANET, AMNET, Bluetooth

### 1

## INTRODUCTION AND METHODOLOGY

The aim of this article is to examine the usability of ad-hoc networks to establish communication among mobile devices by using Bluetooth (Bluetooth™ is a specification for wireless personal area networks (PANs), also known as IEEE 802.15.1 and is developed by the Bluetooth special interest group on <https://www.bluetooth.org>) as a data transmission standard. The results of this study allow further research and help to develop new approaches to use mobile phones as all-in-one devices. Therefore, the evaluation is based on a systematic review of relevant literature and empirical studies related to mobile ad-hoc networks (MANET or mesh networks, e.g. as described by the IETF MANET Workgroup Charter [1, 2]), Bluetooth data transmission and routing between mobile devices as investigated by Zen, Park and Kim in [3].

The focus is to develop a method to transfer data of different categories among mobile devices, for example personalized and anonymous messages without the need to establish a centralised communication structure. This approach allows new applications that make use of the specific network characteristics.

In order to obtain detailed information a prototype software was tested in a simulation environment [4]. The next step was to transfer this setting into reality by studying data transmission in MANETs using Bluetooth on mobile devices. The general idea and the test concept as well as some of the results are presented here.

In Chapter 2 the background of routing in mobile ad-hoc networks is shown. Chapter 3 introduces the concept of AMNETs, a technology used in wireless environments for message transfer. In addition to this, the characteristics of the resulting infrastruc-

ture are discussed. The problem of security is looked at as well. Chapter 4 provides examples for applications that can be created by using AMNET communication. Different classes of data can be transferred and offer services for different classes of recipients, such as category based and address based messaging, anonymous, account based and authenticated message addressees. Chapter 5 discusses further steps and problems.

## 2 BACKGROUND OF ROUTING IN MOBILE AD-HOC NETWORKS

This chapter introduces the main idea of AMNET, an ad-hoc platform for message exchange based on Bluetooth technology, providing very simplistic means of message routing and addressing. AMNET can function as basis for a range of applications which either content with or even profit from its particularities.

There has been a lot of research in routing in MANET [5-7] and the limitations of the routing protocols [8]. Several reactive and proactive routing algorithms are designed for different purposes and network situations, allowing for route discovery either in advance or during packet delivery. Unfortunately, these protocols suffer from a number of shortcomings: Scalability becomes problematic with growing network sizes, performing well only under certain network conditions. The influence of mobility, network load and network topology on performance is described by Broch et al. [9].

There are mobile networks which have to change their topology frequently and continuously due to the rapidly moving nodes, which requires routing discovery techniques to permanently assure valid routes as abstracted by Chlamtac [10]. These networks can be described with the organic term 'vivid', pointing out the vibrant nature of mobile networks.

Vivid MANETs with a large number of mobile nodes are most challenging for ad-hoc routing protocols: In practice, there is a trade-off between route stability and route maintenance bandwidth overhead, and reactive routing algorithms tend not to scale well in large settings. This problem is described in detail in [8, 11]. Conceiving ad-hoc routing protocols that work efficiently in different settings is far from being trivial and has brought up promising combinations of the traditional proactive and reactive paradigms (e.g. Zone Routing Protocol (ZRP) described by Haas et al. in [12]).

## 3 TECHNOLOGY

AMNET describes a networked pseudo-infrastructure which, by design, does not guarantee any service level but relies on the dynamics of the ad-hoc capability of spontaneous message transfer. Although such an approach fails to meet the requirements of a large number of applications, it is a promising foundation for others which have lower requirements towards the networking reliability of the involved communication partners.

AMNET comprises of an ad-hoc store-and-forward message system which is significantly less complex than general MANET data packet networks: data does not need to be forwarded in near real-time, since message delay is acceptable in a store-and-forward system; message routing is significantly more simplistic, since there is no need for real-time route maintenance, and message routing follows a simple broadcast scheme.

AMNET's primary communication layer uses the Bluetooth wireless network suite which is the preferred low-range data exchange method for mobile devices, as mobile phones or PDAs. The user's consent assumed, these widely available and deployed devices form the majority of the AMNET nodes. To bridge the maximum Bluetooth communication range message propagation take place in a delay tolerant environment. This enables multi hop spread of messages even with no direct contact between various nodes.

### Concept of AMNET

Unlike common mesh networks, which strive to provide stable IP-based network connections applicable to all known internet applications and services, we focus on enabling mobile devices for spontaneous exchange of discrete messages by basically using very simple broadcast and store-and-forward techniques. Thus we do not support end-to-end data connections among the nodes, avoiding most of the mesh network complexity and, on the other hand, limiting the use of such a network to applications which can handle these particularities. Factors such as distance in time and space still play an important role in exchanging information from one node to another.

To reflect the differences and similarities of MANET and AMNET we face the features of each concept in the following table.

**Table 1.** Comparison of MANET and AMNET

MANET	AMNET
<b>Routing Features</b>	
Real time packet routing	Delay-able message dispatching
Directed addressing for packets	Messages spread in multicast pattern
Addressing: Defined source and destination	Optional addressing: Category-based message filtering
Proactive/Reactive Routing Protocols	Store-and-forward best-effort ad-hoc transmissions.
Bad performance in vivid networks	Based on vivid networks. Caching concept relies on nodes in action
Typically single-path routing	Multipath approach (according to recipients perception)
<b>Network Characteristics</b>	
Problems in scalability	Scalable: Scaling behaviour is issue of current research*
Creates infrastructure network	Loose pairing of devices: no (or semi-) infrastructure
Consistency of nodes and recipients	Non-consolidatable address space
Network services transparent for application	Offers service profiles: anonymous, authorised, authenticated usage
Precise lossless packet routing	Fish eye routing (compare to [13]), quality-based message drop decisions; random message drop; other optimisation techniques

\* Compared to other ad-hoc networking protocols AMNET-based communication takes place in a local environment and message broadcast is limited by hop-count and caching techniques. Therefore scaling behaviour is not the main interest at this point and is not comparable to the meaning of scaling in IP-based network protocols.

Compared to MANET, the concept of AMNET offers a number of features that do not exist in the common MANET implementations as shown in table 1. Otherwise it lacks some very important features that many common applications rely on. Therefore we analyse what kind of application might profit from the AMNET particularities and name the requirements for developing useful applications in this network environment.

## Application Requirements

In a wireless environment, where mobile nodes build up the network, typical applications can be categorized regarding the user's communication habits. For example, Instant Messaging is a common application with a high potential to be used with MANETs. In this case the following criteria can be considered when trying to achieve a high customer satisfaction:

- Data transmission is beneficial only when a transaction is completed. Concerning completeness of data, the entire message has to be delivered, not only parts of it.
- Concerning time response, message delivery has to be in scope. That means the message should be available in a suitable period of time which allows the user to handle a dialogue.
- The need for proper validity of messages depends on the usage of the instant messaging application. Assuming, validity is not a critical point, we can fulfil customers' needs with other means relying on complex routing procedures.

## Deployed Application Scenarios Equivalent to AMNET

There are existing situations and settings which are built upon the particularities that are pointed out by AMNET implementations. In these applications the problems are addressed specifically. Here are some examples of AMNET principles used in different existing environments:

**Peer-to-peer (P2P) file sharing systems:** A system for distributing information retrieval, called Peer Search introduced by Tang, Xu and Mahalingam in [14], has to overcome the same problems that led us to the consideration of AMNETs. Index flooding can be compared to caching issues and query flooding is opposed by heuristic-based message filtering mechanisms. Like in Peer Search the scalability problem of common MANETs is avoided by using decentralised repositories.

**Cambodian motorbike e-mail:** In remote Cambodian villages, motorbike messengers fetch and deliver e-mails daily, using wireless technology, while passing by rural schools and a central satellite internet uplink. (The Internet by Motorbike; <http://hardware.slashdot.org/article.pl?sid=04/01/30/2144225>.) Sending and receiving messages in a store-and-forward method is a characteristic of AMNET implementations which could connect mobile nodes in isolated environments temporarily.

**Loose sensor networks:** Well known representatives of this type of wireless ad-hoc networks are implementations like smart dust, home monitoring systems, industrial surveillance networks and others. In dense temperature sensor networks for example, the information finds its way throughout the network to a destination and depending on routing implementation the data transferred may be aggregated in order to save capacity of each node, as evaluated in [15].

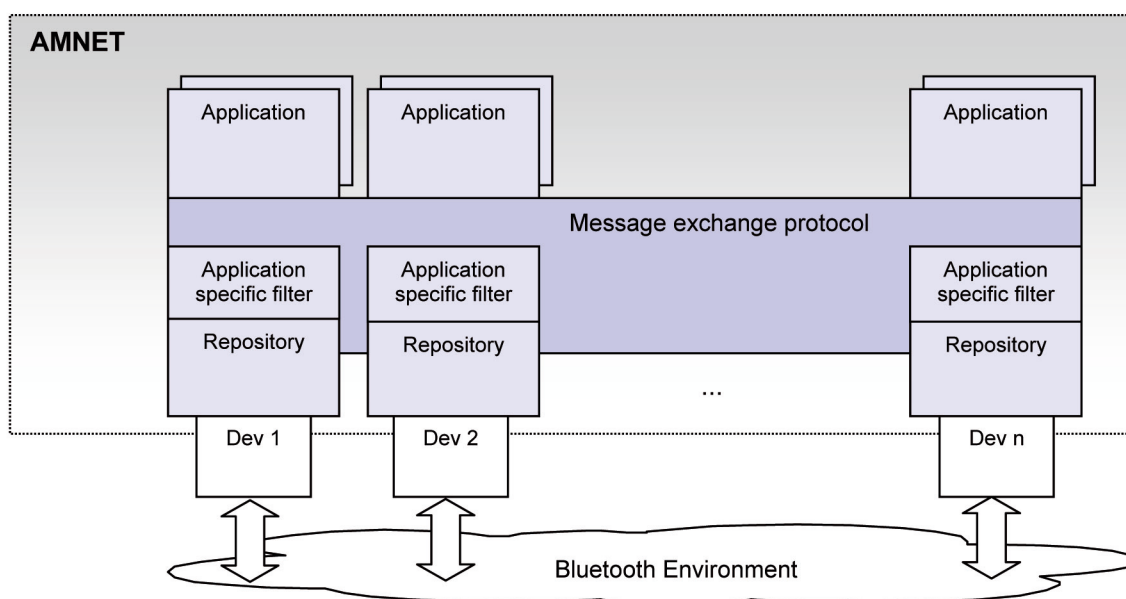
**Locations Based Services (LBS), Who-is-around-lists:** Deployed LBS applications depend on centralised databases providing localised information. In AMNET, LBS could be adopted when accepting a certain degree of haziness, since message validity can be coupled with the count of forwarding nodes, providing a 'proximity-based' information service without the need for central service providers or information repositories.

## AMNET Platform Architecture

In our work we create an AMNET reference implementation using Bluetooth services on mobile phones. The system architecture can be considered a typical layer architecture according to the ISO-OSI reference model. The system architecture affects the network, transport and session layer. Additionally, when content filtering and caching are applied for decisions of the message exchange engine, the application layer contributes to the system as well.

As seen in Figure 1, the AMNET architecture is designed for Bluetooth enabled devices. A repository, combined with application-specific filters, provides message repositories. Message exchange between different devices takes place on top of repositories and filters. Apart from the use of filters, the application itself has no influence on the message exchange process, since this is a task of the underlying message exchange layer. The application cannot rely on messages being sent or received in time.

Figure 1. AMNET platform architecture



Our reference implementation is JAVA based. We use J2ME applications on mobile phones, exploiting the JSR-82 API which allows to interact with the devices' Bluetooth stack. For simulation an interface is developed that allows the use of simulated devices. In our simulation environment we can interact with hundreds of virtually moving devices in order to test routing behaviour.

## AMNET Protocols

The idea of AMNET focuses on one-to-one message transfers that enable devices to send and receive any messages from its neighbours using a store-and-forward pattern. This scenery builds up a network where message caching and time shifted dispatching are used. Even without static connections between source and destination applications can gain advantages using this message network topology. Message transmissions take place regardless of addressing and content.

Messages are cached temporarily to forward them to all close-by neighbours as long as the messages remain valid, according to an invalidating algorithm. Newly received messages are added to this cache if they are not yet stored. Therefore a node uses message multicast according to all the neighbours within a certain period of time in order to synchronise its repositories. This leads to information being copiously spread within the network. To avoid floods, all data is marked with a unique message-ID comprising of a tuple (sender address, message payload hash, hop count). Messages are transferred only over a maximum number of hops.

**Table 2.** AMNET Message Format

General header	Message ID	Application ID	Hops	Time of dispatching
Application header	Category	Address	Validity	
Application data	Message			

Table 2 shows the structure of the message format with its most important fields. A message is separated into three parts: First the general header, containing basic information for taking part in the message exchange process, second the application header, containing application specific information that can be used by the application specific filter to optimise repository maintenance decisions and as the third part the message data itself. The message format consists of three different parts. These parts are assigned to different levels of the architecture seen in figure 1: The general header is analyzed by the message exchange protocol, the evaluation of the application header takes place in the application filter connected to the repository and the message data are passed through to the application.

## Message Filtering

The caching mechanism that builds up the repository is a core feature of the AMNET approach. As AMNET is designed for mobile devices it has to be considered that only a small amount of memory can be used. The implementation of the repository and message cache has to handle these different settings. According to principles of spatial and chronological proximity filters are adopted which reduce the amount of data to be stored to a reasonable size. A common used pattern is to filter out messages that extend certain life-time limitations or covered to many hops.

The filtering concept is even more versatile as far as each application using the AMNET protocol can bring its own filter into the repository in order to enable application specific filtering.

## Devices

Bluetooth is the only technology implemented in a wide range of consumer electronic devices such as mobile phones. It is crucial for our concept of message-spread to enable as many nodes as possible, in order to achieve frequent message exchanges and thus attract more participants with a working service.

Despite other goals in the Bluetooth standard specification, most of the widely deployed Bluetooth implementations in mobile phones merely allow one connection at a time (see [16]). Therefore the proceedings of transactions follow according to time-division-multiplexing methods using store-and-forward.

Working with off-the-shelf mobile phones imposes specific boundaries that limit the size of program code and the memory usage to less than 0.5 MB as described in the CDLC specifications (JSR 139: Connected Limited Device Configuration 1.1 as published by the Java Community process on <http://www.jcp.com>.) and experienced by Huepaniemi et al. in [17].

## Security Issues

Systems that share data in an unknown network environment must address in depth security problems which are known from a range of common internet applications. This includes authorisation, authentication, trusted data transmission and other issues that are needed to guarantee secure transactions in personal messaging sequences.

A new concept to implement security functions in a distributed mobile network is the web-of-trust approach. Web-of-trust (First mentioned in PGP software [22].) is a popular topic of current research and allows security services in distributed network environments without centralised online trust authorities that implement those duties and responsibilities in common network settings [18-20]. As Pirzada and McDonald describe in [21], depending on a central trust authority is an impractical requirement for mobile ad-hoc networks. They present a model for trust-based communication in ad-hoc networks that also demonstrate that a central trust authority is a superfluous requirement.

A web-of-trust model can handle different types of nodes that act not as expected. Deficient nodes have to be bypassed, malicious nodes have to be isolated while warning other nodes nearby and selfish nodes have to be limited in their actions. Thus a powerful model has to cover a range of nodes misbehaviour and consider their direct impact on security aspects.

Since security issues are not the main focus in the field of AMNET research at this point, there is no proof of concept implementation yet. This is part of further development and has to be integrated when the AMNET concept is used in applications and products. (The first available product which implements the AMNET concept including web-of-trust approaches is the EYZE.

ORG platform for mobile messaging and application sharing. See <http://eyze.org/> for more information on the community process that brings up Eyze to work or visit <http://eyze.de> to try out the software)

### 3 APPLICATIONS USING AMNET FOR MOBILE SERVICES

Applications based on the network described can be classified into three groups. The criteria by which the applications are divided into groups are authentication criteria as shown previously. The needed authentication ranges from zero, which means that there is no identification, to full authentication which even fulfils the needs of electronic payment transactions. The authentication and personalisation levels are implemented on top of the presented AMNET data structures, specifically regarding the network protocol.

For each group, an example application which is representative for further application is presented. For the current research, three programs are developed as a proof of concept to show the potentials and to emphasise the abilities of the network.

**Table 3.** Matrix of application categories and identification levels

<b>Anonymous Services</b>	Electronic bulletin board	Advertisements (LBA – location based advertising)	Client server architecture
<b>Account-based Identification</b>	Community features (e.g. who-is-online, who-is-around lists, "Tube Buddies")	File sharing	Web applications/portals
<b>Authenticated Transactions</b>	Traffic jam warnings, emergency calls	E-Payment	VPN, business transactions via internet
	<b>Category based messages (multi hop)</b>	<b>Address based messages (single hop)</b>	<b>Multi hop addressed</b>

Table 3 shows applications assigned to the appropriate group. Note that besides the vertical classification according to the group of assigned identification levels, there is a differentiation of used message types that range from category-based multicast to addressing messages in either single hop or multi hop environments.

Multi hop addressed scenarios are out of research scope concerning the concept of AMNET because there are existing and powerful multi hop addressed routing algorithm that fulfil the needs for these applications better [22, 23]. Therefore we concentrate on multi hop category based messaging and single hop address based messaging. Nevertheless, the store-and-forward mechanism as described earlier allows messages to be spread in a defined range within the network topology. In this context multi hop category based messaging can be understood as a successive message broadcasting in a local area where instead of defined destinations categories are encoded within the message. These allow filter and caching mechanisms to prevent broadcast flooding problems.

The main effort in transferring the research into proof of concept applications is put in three applications that cover a range of different characteristics. They can be assigned to the grey shaded cells in table 3: Electronic bulletin board, who-is-online / who-is-around lists.

#### Electronic bulletin board

An approach to category-based routing and anonymous messaging.

An electronic bulletin board can be used to send messages addressed to all individuals in a specific area (non personal messages). Receiving bulletin messages, called posts, can be restricted by defining different categories which one can subscribe to. For example, an electronic bulletin board can be used to signalise specific interests or offers to other people near-by.

By supporting multiple node hops messages can be sent to a wide range of individuals. Limiting the number of valid hops can be used as an instrument in order to control the range of the local area, where this message can be received..

#### Community Features

Combining who-is-online lists with position based information.

Community services such as configuring a personal profile, using who-is-online lists or complex reputation systems can be provided by mobile ad-hoc networks. One of the most important aspects of these applications is building up a user community [24]. Generating social network effects can be used as one key element to increase diffusion of the described standard. To send a

self-administrated personalized user profile can be used in many ways. For example to meet people with special interests, or to be informed if one of your friends of your who-is-online list is in your current local area.

## Car Traffic Notification Service

Saving lives due to information leap

Imagine a pseudo-intelligent in-car warning system which recognizes an arising traffic jam due to accumulating state messages in the direct environment from many other nodes. In a web-of-trust this information can be forwarded to all nodes taking part in the traffic and thus the driver can be warned in time.

AMNET can contribute to this scenario by providing the loose coupling of nodes and adopting a sophisticated filter system that aggregates all messages and generates warnings to the driver.

# 4

## CONCLUSION

Our research in the field of AMNET suggests that valuable message communication can be introduced for vivid ad hoc networks that serves many applications. This is a realistic alternative for porting all common internet communication features to mobile devices which try to make the insufficiencies transparent for the applications which is an inadequate approach in vivid environments.

The next step in our research on AMNETs is to develop a prototype software which runs in a simulated Bluetooth setting focusing on message propagation and caching mechanisms. We also analyse the network behaviour in crowded as well as in areas with weak nodes density where additional stationary nodes might help to achieve a higher network diffusion in lower time.

Regarding our proof of concept applications the potential for the use of AMNETs can be seen, with further potential for ubiquitous scenarios, as seen in the car-traffic example. Since there are still many open questions, research is extended and contributions from other research groups and companies are used to speed up the design and development of working applications which transfer the AMNET approach into real life products.

## REFERENCES

1. I. I. E. T. Force (2006): "MANET Workgroup Charter", see <http://www.ietf.org/html.charters/manet-charter.html> (15th May 2006).
2. J. Macker and M. Corson (1998): "Mobile ad hoc networking and the IETF," ACM Mobile Computing and Communication Review, vol. 2, pp. 9-14.
3. B. Zhen, J. Park, and Y. Kim (2003): "Scatternet formation of Bluetooth ad networks," Proceedings of the 36th Annual Hawaii International Conference on System Sciences.
4. C. Fuchß (2004): "Synchronization in mobile ad hoc networks," Thesis at University of Potsdam, Department of Computer Science.
5. X. Kaixin, H. Xiaoyan, and M. Gerla (2002): "An ad hoc network with mobile backbones," IEEE International Conference on Communications, vol. 5, pp. 3138-3143.
6. K.-W. Chin, J. Judge, A. Williams, and R. Kermode (2002): "Implementation experience with MANET routing protocols," SIGCOMM Computer Communication Review, vol. 32, pp. 49-59.
7. E. M. Royer and T. Chai-Keong (1999): "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Wireless Communications, vol. 6, pp. 46-55.
8. T. Yu-Chee, N. Sze-Yao, C. Yuh-Shyan, and S. Jang-Ping (2002): "The Broadcast Storm Problem in a Mobile Ad Hoc Network," Wireless Networks, vol. 8, pp. 153-167.
9. J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva (1998): "A performance comparison of multi-hop wireless ad hoc network routing protocols," Proceedings of the 4th annual ACM/IEEE international conference on mobile computing and networking, pp. 85-97.
10. I. Chlamtac, M. Conti, and J. J.-N. Liu (2003): "Mobile ad networking: imperatives and challenges," Ad Hoc Networks, vol. 1, pp. 13-64.
11. H. Xiaoyan, X. Kaixin, and M. Gerla (2002): "Scalable routing protocols for mobile ad hoc networks," Network, IEEE, vol. 16, pp. 11-21.
12. Z. J. Haas, M. R. Pearlman, and P. Samar (2002): "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", see <http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-manet-zone-zrp-04.txt> (20th May 2006).
13. P. Guangyu, M. Gerla, and C. Tsu-Wei (2000): "Fisheye state routing: a routing scheme for ad hoc wireless networks," IEEE Internations Conference on Communications, vol. 1, pp. 70-74.
14. C. Tang, Z. Xu, and M. Mahalingam (2002): "Peer Search: Efficient Information retrieval in Peer-Peer Networks," Hewlett-Packard Labs: Palo Alto.
15. S. Madden, M. J. Franklin, J. Hellerstein, and H. Wei (2002): "TAG: a Tiny Aggregation Service for Ad-hoc Sensor Networks," submitted for review.
16. M. Leopold, M. B. Dydensborg, and P. Bonnet (2003): "Bluetooth and sensor networks: a reality check," Proceedings of the 1st international conference on Embedded networked sensor systems.
17. J. Huopaniemi, M. Patel, R. Riggs, A. Taivalsaari, A. Uotila, and J. van Peurseem (2003): Programming Wireless Devices with Java (TM) Platform, 2nd edition: Addison Wesley Professional.

18. D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong (2002): "Talking to strangers: authentication in ad-hoc wireless networks," Network and Distributed System Security Symposium.
19. P. Michiardi and R. Molva (2001): "A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks", see <http://citeseer.ist.psu.edu/michiardi01core.html> .
20. L. Haiyun, P. Zerfos, K. Jiejun, L. Songwu, and Z. Lixia (2002): "Self-securing ad hoc wireless networks," Proceedings of the 7th International Symposium on Computers and Communications, pp. 567-574.
21. A. A. Pirzada and C. McDonald (2004): "Establishing trust in pure ad-hoc networks," Proceedings of the 27th conference on Australian computer science, vol. 26.
22. K. H. Wang and L. Baochun (2002): "Efficient and guaranteed service coverage in partitionable mobile ad-hoc networks," Twenty-first Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 2, pp. 1089-1098.
23. C. Shigang and K. Nahrstedt (1999): "Distributed quality-of-service routing in ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 17, pp. 1488-1505.
24. C. Lattemann and S. Stieglitz (2005): "A Framework for Governance in Open Source Communities," Proceedings of the 38th Hawaii International Conference on System Sciences.