DESIGN SECURE AND APPLICATION-ORIENTED VANET

Yi Qian, and Nader Moayeri
National Institute of Standards and Technology
100 Bureau Drive, Stop 8920
Gaithersburg, MD 20899-8920, USA

Abstract — **Vehicular ad hoc network (VANET) is recognized as an important component of Intelligent Transportation Systems. The main benefit of VANET communication is seen in active safety systems, which target to increase safety of passengers by exchanging warning messages between vehicles. Other applications and private services are also permitted in order to lower the cost and to encourage VANET deployment adoption. To successfully deploy VANET, security is one of the major challenges that must be addressed. Another crucial issue is how to support different applications and services in VANET. In this paper we propose a secure and application-oriented network design framework for VANET. We consider both security requirements of the communications and the requirements of potential VANET applications and services. The proposed framework consists of two basic components: an application-aware control framework and a unified routing scheme. Besides the network design framework, we further study a number of key enabling technologies that are important to a practical VANET. Our study can provide a guideline for the design of a more secure and practical VANET.**

Keywords: **VANET, security, safety, application-oriented.**

1. INTRODUCTION

To improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the traveling public, Intelligent Transportation Systems (ITS) have been developed, which apply rapidly emerging information technologies in vehicles and transportation infrastructures. The field of inter-vehicular communications (IVC), including both vehicle-to-vehicle communication (V2V) and vehicle-to-roadside communication (V2R), also known as VANET, is recognized as an important component of ITS in various national plans [1]. ITS architecture provides a framework for the much needed overhaul of the highway system infrastructure. The immediate impacts include alleviating the vehicle-traffic congestion and improving operations management in support of public safety goals, such as collision avoidance. Equipping vehicles with various kinds of on-board sensors, and V2V and V2R communication capability will allow large-scale sensing, decision, and control actions in support of these objectives. Communication-based active safety is viewed as the next logical step towards proactive safety systems. These systems provide an extended information horizon to warn the driver or the vehicle systems of potentially dangerous situations in much early phase. The allocation of 75 MHz in the 5.9 GHz band licensed for Dedicated Short Range Communication (DSRC), which supports seven separate channels, may also enable the future delivery of rich multimedia contents to vehicles at short- to medium-range via either V2V or V2R links in VANET [2]. The US Department of Transportation and the automotive industry are aggressively developing DSRC technologies and applications. Their joint effort has identified safety applications enabled by DSRC and evaluated DSRC radio performance [3].

Mobile ad hoc networks (MANET) have been studied for some time, and VANET will form the biggest MANET ever implemented. Therefore, issues of stability, scalability, reliability, and security are of concerns. In VANET, the mobile nodes are vehicles, and because of their high mobility and speed, the main VANET disadvantage is that the network topology changes frequently and very fast. On the contrary, in VANET vehicles move only on predetermined roads, and they do not have the problem of resources limitation in terms of data storage and power. Furthermore, it can assume that it is always possible for a vehicle to obtain its geographic position by using GPS, which can provide good time synchronization through the network as well. In general, good VANET protocol designs should have to be concerned with fast topology changes, as well as different kinds of applications for which the transmission will be established. Moreover, VANET protocols have to reduce the delay, which is very important for safety applications.

In spite of the ongoing academic and industrial research efforts on VANET, many research challenges remain. From the network perspective, security is one of the most significant challenges. In VANET, vehicle safety applications are among its major drivers. Where people's lives are at stake, it is of course essential to secure VANET against abuse. As a special implementation of MANET, a VANET inherits all the known and unknown security weaknesses that are associated with MANET, and could be subject to many security threats. Meanwhile, even as researchers are working on enabling the applications for VANET that have been identified so far, new applications continue to be proposed for VANET.

In this paper, we focus on two major issues in VANET design: security, and support of existing and future VANET applications. In the rest of this paper, we first give a brief background of VANET in Section 2. We then examine the details of the challenges and requirements of VANET design in Section 3, including the general requirements for VANET security and application scenarios. We present our secure and application-oriented VANET design framework in Section 4, followed by a number of important technologies to deploy the proposed framework in Section 5. We give conclusions in Section 6.

2. BACKGROUND ON VANET

In VANET, each vehicle is equipped with the technology that allows the drivers to communicate with each other as well as with roadside infrastructure, e.g., basestations also known as Roadside Units (RSUs), located in some critical sections of the road, such as at every traffic light or any intersection or any stop sign, in order to improve the driving experience and making driving safer. By using those communication devices known as On-Board Units (OBUs), vehicles can communicate with each other as well as with RSUs. VANET is a self-organized network that connecting the vehicles and RSUs, and the RSUs can be connected to a backbone network, so that many other network applications and services, including Internet access, can be provided to the vehicles.

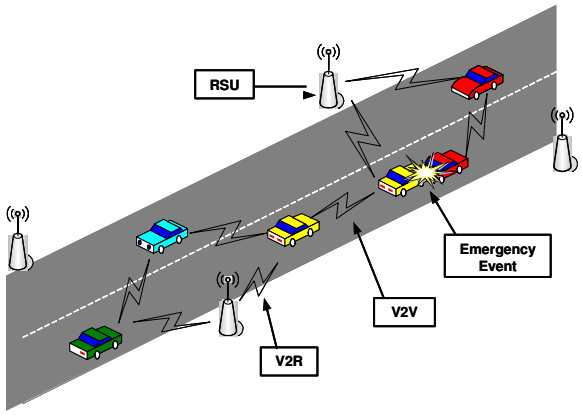

Figure 1. An Example of VANET

The U.S. Federal Communications Commission (FCC) recently has allocated 75 MHz of DSRC spectrum at 5.9 GHz to be used exclusively for V2V and V2R communications [2]. The primary purpose is to enable public safety applications that save lives and improve vehicular traffic flow. Private services are also permitted in order to lower cost and to encourage DSRC development and adoption. The DSRC spectrum is divided into seven 10 MHz wide channels as shown in Figure 2. Channel 178 is the control channel, which is generally restricted to safety communications only. The two channels at the edges of the spectrum are reserved for future advanced accident avoidance applications and high-powered public safety usages. The rest are service channels and are available for both safety and non-safety application.

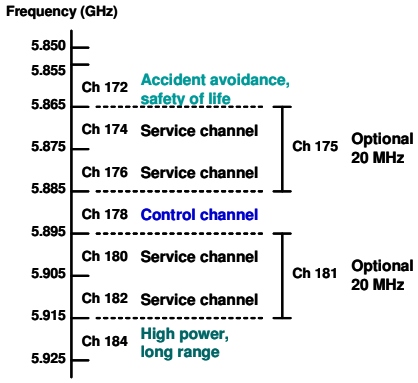

Figure 2. DSRC Channel assignment in North America

The IEEE has completed the standards IEEE P1609.1, P1609.2, and P1609.4 for vehicular networks and recently released them for trial use [4]. A fourth standard, P1609.3 is still under further development. P1609.1 is the standard for Wireless Access for Vehicular Environments (WAVE) Resource Manager. It defines the services and interfaces of the WAVE resource manager application as well as the message data format. It provides access for applications to the other architecture. P1609.2 defines security, secure message formatting, processing, and message exchange. P1609.3 defines routing and transport services. It provides an alternative to IPv6. It also defines the management information base for the protocol stack. P1609.4 deals mainly with how the multiple channels specified in the DSRC.

The WAVE stack uses a modified version of the IEEE 802.11a, known as IEEE 802.11p [5], for its Medium Access Control (MAC) layer protocol. It uses CSMA/CA as the basic medium access scheme for link sharing and uses one control channel to set up transmissions, which then should be done over some transmission channels. At the PHY layer, 802.11p is expected to work in the 5.850 – 5.925 GHz DSRC spectrum in North America, which is a licensed ITS Radio Services Band in the United States. By using the OFDM system, it provides both V2V and V2R wireless communications over distances up to 1000 m, while taking into account the environment, that is, high absolute and relative velocities (up to 200 km/h), fast multipath fading and different scenarios (rural, highway, and city). Operating in 10 MHz channels, it should allow data payload communication capabilities of 3, 4, 5, 6, 9, 12, 18, 24, and 27 Mb/s. By using the optional 20 MHz channels, it allows data payload capabilities up to 54 Mb/s.

As the overall DSRC communication stack between the link and application layers is being standardized by the IEEE 1609 Working Group, the overall DSRC communication architecture in the draft IEEE 1609 standard contains two parallel stacks: one for TCP/IP-based communications and the other for safety messaging.

For safety messaging, the amount of information to be transmitted is relatively small, but the transmission reliability as well as the latency and packet dissemination are of great importance.

3. CHALLENGES AND REQUIREMENTS IN VANET DESIGN

In the previous section we provide a brief review of VANET background. In reality, to successfully deploy VANET, a number of challenging issues must be addressed. In the following we focus on two major issues in network layer design: security, and support of existing and future VANET applications. In the rest of this section we first discuss the common requirements of security in VANET and possible attacks to VANET. We then address the current and potential applications of VANET.

3.1. SECURITY CHALLENGES IN VANET

VANET poses some of the most challenging problems in wireless ad hoc and sensor network research. In addition, the issues on VANET security become more challenging due to the unique features of the network, such as high-speed mobility of network entity or vehicle, and extremely large amount of network entities. In particular, it is essential to make sure that "life-critical safety" information cannot be inserted or modified by an attacker; likewise, the system should be able to help establishing the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers and passengers. It is obvious that any malicious behavior of users, such as a modification and replay attack with respect to the disseminated messages, could be fatal to other users.

In the past few years, considerable effort has been spent in research on VANET networking protocols and applications. However, research on security threats and solutions and reliability of VANET only started recently, e.g., [6-11]. Summarizing from the recent researches above, VANET security should satisfy the following requirements: message authentication and integrity, message non-repudiation, entity authentication, access control, message confidentiality, availability, privacy and anonymity, and liability identification.

Message Authentication and Integrity: Message must be protected from any alteration and the receiver of a message must corroborate the sender of the message. But integrity does not necessarily imply identification of the sender of the message.

Message Non-Repudiation: The sender of a message cannot deny having sent a message.

Entity Authentication: The receiver is not only ensured that the sender generated a message, but in addition has evidence of the liveness of the sender.

Access Control: Access to specific services provided by the infrastructure nodes, or other nodes, is determined locally by policies. As part of access control, authorization establishes what each node is allowed to do in VANET.

Message Confidentiality: The content of a message is kept secret from those nodes that are not authorized to access it.

Availability: The network and applications should remain operational even in the presence of faults or malicious conditions. This implies not only secure but also fault-tolerant designs, resilience to resource depletion attacks, as well as survivable protocols, which resume their normal operations after the removal of the faulty participants.

Privacy and Anonymity: Conditional privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, position, and traveling routes along with their relationships, has to be protected; while the authorities should be able to reveal the identities of message senders in the case of a dispute such as a crime/car accident scene investigation, which can be used to look for witnesses.

Liability Identification: Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system. As part of the "conditional privacy" above, the authorities should be able to reveal the identities of message senders in the case of a dispute such as a crime/car accident scene investigation, which can be used to look for witnesses.

Several attacks have been identified that can be classified depending on the layer the attacker uses. At the physical and link layers the attacker can disturb the system either by jamming or overloading the channel with messages. Injecting false messages or rebroadcasting an old message is also a possible attack. The attacker can also steal or tamper with a car system OBU or destroy a roadside unit, RSU. At the network layer the attacker can inject false routing messages or overload the system with routing messages. The attacker can also compromise the privacy of drivers by revealing and tracking their positions. The same attacks can also be achieved using the application layer. In the following, we summarize the major vulnerabilities and security threats of VANET.

Jamming: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the VANET scenario, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.

Impersonation: An attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. An adversary can also impersonate roadside units, spoofing service advertisements or safety messages. So an impersonator can be a threat. Message fabrication, alteration, and replay can all be used towards impersonation.

Privacy Violation: The collection of vehicle-specific information from overheard vehicular communications will be very easy with VANET deployed. Then inferences on the personal data of drivers could be made, thus violate the privacy of drivers.

Forgery: An attacker can forge and transmit false hazard warning information or other messages, and it can rapidly contaminate the large portions of the VANET coverage area. The correctness and timely receipt of application data is a major vulnerability.

In-transit Traffic Tampering: A node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages. Attackers can also replay messages, e.g., to illegitimately obtain services such as traversing a toll check point. Tampering with in-transit messages may be simpler and more powerful than forgery attacks.

On-board Tampering: The attacker may select to tinker with data, e.g., velocity, location, status of vehicle parts at their source, tampering with the on-board sensing and other hardware. In fact, it may be simpler to replace or by-pass the real-time clock or the wiring of a sensor, rather than modifying the binary code implementation of the data collection and communication protocols.

3.2. VANET APPLICATIONS

In the previous discussion we address the network design issue from the security perspective. In practice, a good system design also depends on understanding the applications that will be carried in the network. These applications not only call for diverse solutions, such as bandwidth, delay, security, and reliability, but also demonstrate different communication patterns, such as one-to-one, one-to-many, many-to-one, and many-to-many. However, most existing wireless network architectures could not efficiently support such demands. Therefore, it becomes a major challenge to support and enable diverse applications and services.

Here we summarize the existing applications and several potential applications that have been proposed for VANET. It is important to note that we also elaborate on the functions of each application that shall be provided in the MAC layer and the network layer, so as to fulfill the requirements of these applications.

VANET would support life-critical safety applications, safety warning applications, electronic toll collections, Internet access, group communications, roadside service finder, etc.

Life-Critical Safety Applications: e.g., Intersection Collision Warning/Avoidance, Cooperative Collision Warning, etc. In the MAC Layer, the Life-Critical Safety Applications can access the DSRC control channel and other channels with the highest priority. The messages can be broadcasted to all the nearby VANET nodes.

Safety Warning Applications: e.g., Work Zone Warning, Transit Vehicle Signal Priority, etc. The differences between Life-Critical Safety Applications and Safety Warning Applications are the allowable latency requirements, while the Life-Critical Safety Applications usually require the messages to be delivered to the nearby nodes within 100 milliseconds, the Safety Warning Applications can afford up to 1000 milliseconds. In the MAC Layer, the Safety Warning Applications can access the DSRC control channel and the other channels with the 2^{nd} highest priority. The messages can be broadcasted to all the nearby VANET nodes.

Electronic Toll Collections (ETCs): Each vehicle can pay the toll electronically when it passes through a Toll Collection Point (a special RSU) without stopping. The Toll Collection Point will scan the Electrical License Plate at the OBU of the vehicle, and issue a receipt message to the vehicle, including the amount of the toll, the time and the location of the Toll Collection Point. In the MAC layer, the Electronic Toll Collections application should be able to access the DSRC service channels except the control channel, with the 3^{rd} highest priority. It should be a direct one-hop wireless link between the Toll Collection Point and the vehicle.

Internet Access: Future vehicles will be equipped with the capability so that the passages on the vehicles can connect to the Internet. In the MAC layer, the Internet Access applications can use DSRC service channels except the control channel, with the lowest priority comparing with the previous applications. In the network layer, to support VANET Internet access, a straightforward method is to provide a unicast connection between the OBU of the vehicle and a RSU, which has the link toward the Internet.

Group Communications: Many drivers may share some common interests when they are on the same road to the same direction, so they can use the VANET Group Communications function. In the MAC layer, the Group Communications can use DSRC service channels except the control channel, with the lowest priority comparing with the safety related applications and ETCs. In the network layer, to support such application scenario, multicast is the key technology. In the past, Internet multicast has not been successful due to its complexity and, more important, because Internet multicast requires global deployment, which is virtually impossible. In a VANET, however, since all nodes are located in a relatively local area, implementing such group communication becomes possible.

Roadside Services Finder: e.g., find restaurants, gas stations, etc., in the nearby area along the road. A Roadside Services Database will be installed in the local area that connected to the corresponding RSUs. In the MAC layer, the Roadside Services Finder application can use DSRC service channels except the control channel, with the lowest priority comparing with the safety related applications and ETCs. Each vehicle can issue a Service Finder Request message that can be routed to the nearest

RSU; and a Service Finder Response message that can be routed back to the vehicle.

In short, the application layer requirements must be addressed in the MAC layer and network layer design. In the next section we provide a network design framework to satisfy the above applications while providing sufficient security.

4. NETWORK DESIGN FRAMEWORK

In this section we elaborate on a network design framework to address the security requirements in VANET, and fulfill the demands of existing and future applications discussed above.

4.1. COMPONENTS

In this framework there are two major components.

Application-Aware Control Scheme – To efficiently support different applications, the network control scheme shall be aware of the availability of different applications. In general, the application can be either located in a single node (RSU or OBU) or distributed in multiple nodes (RSUs and/or OBUs) in the VANET. To provide these applications, the servers must register the type and availability of applications to the control framework. Moreover, the availability information shall be updated periodically or based on predefined events. Upon receiving these messages, the control framework will also be responsible for distributing such message to nodes in the VANET.

Unified Routing Scheme with Security Requirements – With the availability information of the application, a unified routing scheme shall be designed such that all the applications discussed in the last section shall be supported. The packets of a certain flow will be forwarded based on the application and the security requirements.

4.2. CASE STUDIES

To illustrate the behaviors of the framework, we use the following cases as examples.

Case 1 – All the OBUs and RSUs have been registered for the safety related applications (Life-Critical Safety Applications, and Safety Warning Applications) in the control framework. The safety related application messages will be sent to all the nearby VANET nodes through broadcasting. The safety related application messages do not have to be encrypted, i.e., it does not need to satisfy the message confidentiality requirement, but it must have to satisfy the message authentication and integrity, message non-repudiation, entity authentication requirements. Security mechanisms must be in place to against in-transit traffic tampering.

Case 2 – For the OBUs registered for the Electronic Toll Collections in the control framework. Each ETC related application message is a one-hop wireless link between the Toll Collection Point and the vehicle. The ETC related application messages need to satisfy the message confidentiality, message authentication and integrity, message non-repudiation, and entity authentication requirements.

Case 3 – Assume that each RSU has been registered as the gateway for Internet access in the control framework. Now suppose a regular best-effort Internet access request from an OBU arrives at the control framework; a single-path unicast routing scheme between the OBU and a nearby RSU can be set up for such a request. Notice that in such a scenario, the single path routing scheme cannot defend compromised OBUs in a multihop situation. Security mechanisms must be in place to against in-transit traffic tampering.

Case 4 – For the OBUs that registered for Group Communications in the control framework, multicast is used to realize the application. In such a case, security mechanisms must be in place to ensure the security of the multicasting in VANET. While the security of multicasting in MANET have been studied for a while, e.g., [13, 14], secure multicasting schemes in VANET still need to be addressed.

Case 5 – For the OBUs that registered for Roadside Services Finder application in the control framework, a unicast path can be set up between the requesting OBU and a nearby RSU. Same security mechanisms need to be in place as those of Case 3.

5. ENABLING TECHNOLOGIES

To deploy the proposed framework, a number of key technologies must be addressed. In the rest of this section we discuss these issues, including security management, key management, secure routing and network coding.

5.1. SECURITY MANAGEMENT

In the proposed framework the security management scheme is very important to the system. Similar to [15], we consider the security management scheme responsible for monitoring the operation of the VANET and quickly identifying possible security attacks and threats.

5.2. KEY MANAGEMENT

In addition to the MAC layer, key management is also important to the network layer. To provide a secure communication channel between any two nodes in a VANET, it is important to develop a key management scheme to establish a unique key for each session. Another potential research topic in key management is the key distribution scheme for group communications. One simple solution for group communication is to utilize a single group key. However, such an approach is not efficient because of two factors: the key will be exposed if a single group member is compromised; and the communication overhead will become a big burden if a member can frequently join or leave the group, a typical scenario for a

system like VANET with mobile nodes. More work need to be done on the topic of key management for VANET.

5.3. SECURE ROUTING AND NETWORK CODING

Secure routing has been discussed for MANET in a number of previous studies (e.g., [16]). However, we notice that none of them fully address the scenarios of VANET applications discussed in the previous section. To address the secure routing issue, we believe that the emerging network coding technique should be applied because it can provide the optimum solution and reduce the computational complexity for many problems [17]. Our recent work reveals that we can incorporate the security and reliability requirements into network coding design. With the proposed design guidelines on MANET [18], we can see that the network coding approach can be utilized to improve both the security and the reliability as follows. First, the network coding scheme can be designed in a way that none of the intermediate nodes can decode the original message. In this manner, an adversary may not be able to overhear the whole message unless it is near to the source or destination of a connection. Second, the coding scheme can be designed such that the destination can still correctly decode the original message even if some data are dropped in the network, and if some data are modified deliberately by intermediate nodes. In For future work, we will explore the details of netwok coding schemes for VANET design.

6. CONCLUSIONS

VANET is a promising wireless communication technology for improving highway safety and information services. In this paper we propose a secure and application-oriented network design framework in which both security concerns and the requirements of potential VANET applications are taken into account. We also study several enabling technologies for the design framework. These enabling technologies include security management, key management, secure routing and network coding. We believe that our study can provide a guideline for the design of a more secure and practical VANET.

REFERENCES

[1] U.S. Department of Transportation, Intelligent Transportation Systems (ITS) Home, http://www.its.dot.gov/index.htm

[2] Dedicated Short Range Communications (DSRC) Home. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[3] Crash Avoidance Metric Partnership, "Vehicle Safety Communication Project Final Report", available through U.S. Department of Transportation.

[4] IEEE Draft P1609.0/D01, February 2007.

[5] IEEE Draft P802.11p/D2.0, November 2006.

[6] P. Papadimitratos, V. Gligor, J-P. Hubaux, "Securing Vehicular Communications – Assumptions, Requirements, and Principles", Proceedings of the Workshop on Embeded Security on Cars (ESCAR) 2006, November 2006.

[7] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, October 2006.

[8] Tim Leinmuller, Elmar Schoch, and Frank Kargl, "Position Verfication Approaches for Vehicular Ah Hoc Networks", IEEE Wireless Communications, October 2006.

[9] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Priviate Vehicular Communications", Proceedings of the 7th International Conference on ITS Telecommunications, June 2007.

[10] Maxim Raya, and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, Vol.15, No.1, pp.39-68, 2007.

[11] Tim Leinmuller, Elmar Schoch, and Christian Maihofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks", Proceedings of Forth Annual Conference on Wireless on Demand Network Systems and Services, 2007.

[12] Qing Xu, Raja Sengupta, Tony Mak, and Jeff Ko, "Vehicle-to-Vehicle Safety Messaging in DSRC", Proceedings of VANET'04, October 2004.

[13] Haibing Mu, Yun Liu, and Changlun Zhang, "A Composite Multicast Key Management Scheme for MANET", Proceedings of 6th International Conference on ITS Telecommunications, Page(s):794 – 797, June 2006.

[14] Tzu-Chiang Chiang; Yueh-Min Huang, "Group keys and the multicast security in ad hoc networks", Proceedings of 2003 International Conference on Parallel Processing Workshops, Page(s):385 - 390, 6-9 Oct. 2003.

[15] N. Ben Salem, and J.-P. Hubaux, "Securing wireless mesh networks", IEEE Wireless Communications, Vol.13, No.2, pp.50-55, April 2006.

[16] Hongmei Deng, Wei Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, Vol.40, No.10, pp.70-75, October 2002.

[17] D. S. Lun, N. Ratnakar, M. Medard, R. Koetter, D. R. Karger, T. Ho, E. Ahmed, and F. Zhao, "Minimum-cost Multicast over Coded Packet Networks", IEEE Transactions on Information Theory, Vol.52, No.6, pp.2608-2623, June 2006.

[18] Kejie Lu, Shengli Fu, and Yi Qian, "On the Design of Future Wireless Ad Hoc Networks", Proceedings of IEEE GLOBECOM'2007, November 2007.