ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 81-86 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

Trusted dissemation of data in Opportunistic Network

Humna Mumeed ,Naveed Farhana, Mohammed Niyaz Ullah

Department of CSE,Keshav memorial institute of tech,India, i_humul11@yahoo.in
Department of CSIT, Taif University, KSA, farhana_naveed@rediffmail.com
Department of ECE,Islamia College of engineering &tech,India, niyaz@netzero.com

Abstract— Recent advances in the field of computer network and wireless communication technologies, so called opportunistic networks is been materialized. Opportunistic network has many potential applications, from home security to the human preparedness. This paper considers a human aspects of trust , privacy and security on the performance of the opportunistic network, different research papers in the related fields are surveyed and proposed the solutions on this aspects.

Keywords-opportunistic network; trust; privacy; security

I. INTRODUCTION

With the rapid evolution of network diversity and the development of short range wireless communication technologies, a new network known as opportunistic networks emerges[1], this kind of network falls into two fields- Mobile Ad-hoc Network (MANET)[3] and Delay Tolerant Network (DTN)[1].

Opportunistic network thus comprises the methods and features of Delay or Disruption Tolerant Network. They are very much suitable to support the pervasive networking scenario, in which a huge number of devices carried by users and embedded in the environment communicates wirelessly without requiring any pre-existing infrastructure. By enabling end to end connectivity and hence communication without requiring complete paths, opportunistic networks are much closer to real pervasive networking scenarios, with respect to the legacy MANET paradigm.

An opportunistic network consists of nodes. These nodes are typically handheld devices carried by people which are equipped with large memory, good sensing capability, high computational power with short-range radio transmission functionality and wirelessly connected to each other[2]. An opportunistic network node can be either mobile or fixed. A mobile node is a mobile device carried by humans such as a Bluetooth or Wi-Fi enabled mobile phone or PDA. A fixed node, working as an access point, is a device set in certain locations to disseminate information to mobile nodes. Implemented with the same data sharing protocol, a node enabled with opportunistic network applications is capable of discovering other nodes, automatically and communicate without any user intervention. The transmission range between two connected nodes is usually short. Message forwarding in opportunistic networks is based on one-hop message exchange. When nodes get into each other's transmission range, contacts will appear opportunistically. That is why the performance of the network depends on the mobility of nodes. Whenever information is stored in the fixed nodes or has been spread to some mobile nodes, they will start to disseminate it to others.

Due to the new and attractive characteristics of opportunistic networks, a convenient way for people who do not know each other to share and disseminate information becomes easier. Wireless devices within transmission range will make contacts opportunistically and search information that matches their user's interests. If matching information is found, they will download it spontaneously for later use. For instance, when you are wandering in a shopping mall and wondering where to find new fashion styles of clothes on show or good bargains for this week, a message may have already been sent to your mobile phone to update with latest information. You may get the message from any corner of the shopping mall where people exist or from an access point, and spread it to others when you are moving on the way. we can also define which kind of information you would like to search and obtain.

In opportunistic network, spontaneous interaction and collaboration among prior unknown nodes and user provides his/her device as a network node resulting in two types of collaboration between the nodes called as active and passive collaboration.

The nodes help users become aware of each other and stimulate face-to-face conversation is known as active collaboration. Also, autonomous nodes communication for sharing information without user interaction is possible, i.e., nodes pass information to other nodes in their vicinity (passive collaboration). Both, active and passive collaboration requires a user to specify what kind of information he offers and what kind of information he is interested in, and collaboration raises questions concerning three important human aspects-trust, user privacy and security, that could influence users and rely on the opportunistic network. Users have always been concerned about their privacy. Trust is a major concern as users will be making their devices available for application tasks that may not even pertain to them. Likewise they will be using virtually unknown devices for their own tasks. Security

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 81-86 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

guarantees that communications made over the opportunistic network are secure enough that no one other than the sender or the receiver could access the content of them. We discuss trust based on user behavior in the next section, and present privacy preservation techniques in section III. We discuss our security and privacy challenges in section IV. In section V we conclude and discuss future scopes of the opportunistic network.

II. TRUST

Trust has been researched for the past few years, with some encouraging results in other types of distributed systems. A trust value is assumed to be very similar to the human notion of trust. Before a node in a network agrees to interact with another, it gathers information about the other node, and determines a trust value depending on previous collaborations with this particular device or class of devices, on reputation values provided by third devices and other application dependent data. This trust value can be applied to access control problems (is the device trusted enough for it to be allowed access to a resource?), to ensure confidentiality (can it see this piece of information?) and similarly to other security problems.

Trust in general has been researched since the early 70's [4], and applied to computing in the early 90's [5]. It is of course probabilistic in nature, so it is not applicable as the only security measure in high security systems, but it gives good results e.g. in multi-agent systems when used to significantly decrease the probability of a harmful interaction with a malicious agent [6]. And from there, it is a short way to applying trust to opportunistic networks in a similar fashion.

However, the application of trust values presents a unique challenge in the case of opportunistic networks, In many trust models in the literature, trust relies to some extent on data that can be collected externally. Example, in many trust models concerning pervasive systems, a user, apart from assessing the trust into a file provider from his own experiences, can contact other users about their opinion of the provider, to assess the provider's reputation. If necessary, the user can wait for some amount of time for the opinions of other users to arrive. In the case of opportunistic networks, all information that should be used must be locally and immediately available, considering that the durations of contacts are very short. Hence, reputation values in their pure form, a major source of trust information in other models, can't be used in opportunistic network.

Now there are many application areas in which trust can be applied in conjunction with opportunistic networks. For example, one might think of a network in which everyone can dispatch a query ("Who currently sells a used vehicle, model A, price up to B?"), and wait for replies, this way sparing themselves the reading of many sale ads in newspapers, and possibly reaching previously unknown sellers. After getting replies, they would check the offers and rate the offers according to satisfaction for future reference for other users, and buy the best possible option. This is the standard model of providing and using recommendations in a trust framework, similar to that on eBay, and the components (dissemination, routing and trust metrics in opportunistic networks) are relatively well researched.

However, the locality of communication gives rise to more than a challenging problem. As mentioned before with respect to trusted authorities, interactions in such networks can't be observed by an entity outside the connectivity range of the communicating parties. This means that opportunistic networks are inherently sensitive to user behavior, since they rely on user devices behaving in a way that will benefit others, and this kind of good behavior cannot be monitored or enforced directly. For example, if a large set of nodes rely on other nodes to forward their messages, but are not willing to forward messages themselves, the routing network quickly breaks down.

There has been research works which investigates that how egoistic behavior affects the utility of an opportunistic network. In [7], authors proposed a setup for opportunistic network in which each node has iHave and iWish lists (with the obvious semantics), and on each encounter they exchange data that the one has and the other wishes for. The authors investigate in how far it affects the system when there are nodes that only collect data from other devices, but don't share anything, and clearly this behavior has been found to negatively influence the network utility.

Egoistic behavior has to be taken seriously, as a study concerning a file sharing application found. A user behavior study from 2005, [8], has collected data about the usage of the file sharing application Gnutella, and found that about 85% of users share no files at all, using the system egoistically only for downloading and not for uploading, and that this number has increased from 66% in 2000. On the internet, it is relatively easy to set a requirement that can counter egoistic behavior, e.g. in Gnutella anyone wishing to download something may have to have an account with a minimal number of uploads. In opportunistic network behavior is not only indirectly controllable, it is invisible to anyone who isn't situated in the nearest vicinity.

Imagine an opportunistic network which is designed to disseminate messages, with the constraint set by the message originator that they should only be given to entities with a trust value above a certain threshold. Is it possible to guarantee or at least encourage users to actually apply this trust value when disseminating the message, given that the trust value is computed on behalf of another entity, and not for the node's own security? In other words, if users are egoistic enough to use resources and not to

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 81-86 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

provide any as in Gnutella, they are quite likely not to apply security constraints on behalf of other entities.

It is important to focus on investigating various aspects of the effect of user behavior on trust based security in opportunistic networks, i.e. in how far this behavior reduces the effectiveness of a trust value, and how to devise ways to counter this effect, or even provide control over dissemination behavior that would encourage users to behave in a way which benefits the network. This is a challenging problem given that the message originator does not even know the nodes that the message will be passed through in an opportunistic network, and there is no way of controlling the transmission itself while it is ongoing. Even conceptually, it is more challenging than participation incentive schemes, since it is an attempt to make users behave in a particular way when participating, rather than just convincing them to passively make their resources available. On the other hand, it is an idea that would be very rewarding when implemented, since the possibility of encouraging users to apply a globally administered security measure would guarantee a significantly more stable and trusted system, while still retaining the Ad-hoc nature of the network with all its properties. With the inherent instability that is caused by user behavior removed, an Ad-hoc network[9] becomes easier to reason about, theoretical results become more applicable, and a practical deployment becomes more feasible.

III. PRIVACY

The mobile devices in Opportunistic Networks are carried by humans. The communication occurs in the users proximity, the fact that information passes from his device or to his device might conflict with the user's privacy. Privacy is the ability of a user to prevent information about him or her from becoming known to other users. If a user expresses interest in some kind of information or provides information or knowledge to other users/devices in the vicinity, there is a danger that other users exploit this information.

Opportunistic network nodes are similar to RFID tags in the sense that they communicate with their surroundings without user interaction. They also store personal data and interests. Therefore, mechanisms for preserving user privacy are needed.

Some of the research has been done previously by different researchers in the related field can be applicable to the opportunistic network, in [10][11] the authors presents concepts which may be useful when constructing tools to enable individuals to express a personal location privacy policy. Its idea is that the individual should be able to adjust the accuracy of his location, identity, time and speed, and therefore have the power to enforce the need-to-know principle. The accuracy is dependent on the intended use of the data, and the use in turn is encoded within privacy policies.

Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks[12] is another scheme which describes the scenario of a battlefield in mind in which routing with Untraceable Routes for Mobile Ad-hoc Networks route anonymity and location privacy. The intention is that packets in the network cannot be traced by any observing adversary. Additionally, this routing scheme provides inability of linkage. Prior to one node's ability to send a message to another, a route must be established through route discovery. This route discovery is achieved by broadcasting and forwarding packets. The sender of a message is anonymous, because it is impossible to judge whether a node is actually sending a message it generated or is simply forwarding a packet as part of a route.

In [15] author proposed an application of mix network and their system, the scheme does not keep the identity – telephone number – of the recipient anonymous. Only the location of the recipient is protected. Remarkably, their system remains secure even if all intermediate nodes are observed by an adversary.

In[13] [14] an approach is proposed in which it is somewhat similar to mix networks. In these networks, the infrastructure provides an anonymity service. The infrastructure delays and reorders messages from subscribers within a mix zone to confuse an observer. One problem with this system is that there must be enough subscribers in the mix zone to provide an acceptable level of anonymity.

Anonymous usage of location based [15] mechanism called cloaking that conceals a user within a group of k people. They consider a user as k-anonymous if and only if, he is indistinguishable from at least $k - 1$ other users. To achieve this, the accuracy of the disclosed location is reduced. Then, any of the people within the disclosed area could have been the particular user resulting in the reducing the accuracy of disclosure timestamps.

With respect to user privacy preservation in opportunistic networks, none of the above mechanisms are fully suitable. This is due to the fact that privacy preserving mechanisms are tailored to the considered applications. However, all approaches teach a fundamental lesson, in order to preserve user privacy, the source, i.e., the user's identity, of an event or information has to be obfuscated from an observer.

Other solution which is directly applicable to opportunistic network is to separately keep the private and public areas within the device or network.

Some other techniques proposed by [16] which can be directly applicable by protecting the privacy of nodes by characterizing them into anonymity or pseudonymity.

- Providing algorithms for detecting malevolent opportunistic network(bad), which masquerade as benevolent opportunistic networks(good) in order to attack prospective nodes. Detection will deny them opportunity to compromise privacy of nodes

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 81-86 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

- Developing methods to protect opportunistic networks against all kinds of privacy attacks, and to disable malicious uses of opportunistic networks for privacy attacks.

IV.SECURITY

As there is no centralized authority can be used as a trusted third party because it won't be accessible locally. This is a considerable restriction. The lack of a central authority means that cryptographic signatures, many authentication protocols and encryption algorithms are not applicable. As we have discussed earlier that opportunistic network falls into two fields as delay tolerant network and mobile Ad-hoc network and also the epitome of pervasive networking whose critical problems are privacy and security. So few concepts of pervasive computing[17] can be applied to opportunistic network. Some of the privacy and security challenges and their perspective solutions has been discussed below by surveying the various research papers in the field of pervasive computing and mobile Ad-hoc network.

Message forwarding can be done between the nodes which are trustworthy and maintaining the list of trusted nodes, using a route that passes through only trusted devices (or as many trusted nodes as possible) is challenging. Numerous research papers have been written on individual Ad-hoc routing protocols. A survey of secure wireless Ad-hoc routing can be found in [18]. Secure wireless Ad-hoc routing protocol most relevant to opportunistic network is discussed in[19].It is an on-demand protocol that works in the presence of compromised nodes. It uses symmetric cryptography. It authenticates routing messages using one of the three schemes:

- Sharing secret information between the nodes.
- Shared secrets between communicating nodes combined with broadcast authentication.
- Digital signatures.

The proposed secure routing protocols in wireless or Ad-hoc networks cannot be used directly in opportunistic networks because they are highly heterogeneous in nature. Their nodes have different processing abilities, power sources, modes of transmission (wired or wireless).

Maintaining the privacy of nodes, means data privacy or confidentiality. Opportunistic networks can be feasible only if privacy of nodes are guaranteed. Privacy of nodes can be guaranteed by its access control(authentication and authorization). Its intrusion prevention (using security primitives, relying on trust, secure routing etc.).The problem of guaranteeing access control and performing real-time intrusion detection for opportunistic networks are more difficult than for the Internet, wireless or Ad-hoc networks because of the highly heterogeneous nature of participating devices and the spontaneous manner in which they are formed.

Another security solution is that messages in opportunistic network might be sent from one node to another node(peer to peer), or there can be intra-cluster communication among devices in some specific area. A local cluster head (a trusted device doing an extra job) can use public key cryptography while communicating with its neighbors. A cluster head can announce its public key. Nodes can encrypt data with the public key and, upon receiving encrypted data, the cluster head can decrypt them with its private key. But a malicious device can pose as a cluster head and can distribute its own public key. So, this approach will not work if the cluster head cannot exclude such 'competition' in distributing its forged public key.

If a node that needs help and it sends request to the another node which can provide help to needy node but malicious node in the path, instead of forwarding it might inform the person that help is on the way. It could also tamper the messages.

The possible solution to this the needy can send redundant messages to the through multiple neighbors. This will increase the chances that atleast one of the multiple message copies will reach the destination, even if there are attackers on some paths. So, redundancy of routes can be exploited to avoid the attackers.

Denial of service attacks by malicious devices or nodes is the frequent and wrong requests for help. This problem can be solved by keeping, upper limit can be applied to the number of requests any device can be made. Thus, it will limit the number of times any device can send a false help request. In addition, the rescue team can attempt contacting the requester to confirm an emergency request.

Sometimes Denial of Service (DOS) attack can be done to weak devices such as mobile/cell phones, identifying the week device and identifying their resources and compensating in case of the attacks is the major challenge for the opportunistic network.

A malicious device capable of masquerading can generate requests with multiple IDs, resulting in many false alarms. Services that need authentication can be misused if their IDs can be spoofed. A device capable of spoofing ID of a trusted node or a node with critical functions can pose many kinds of attacks.

It is difficult to guarantee that malicious nodes will not join the opportunistic networks, nodes can monitor their neighbors for possible attempts of ID spoofing. The SAVE protocol [20]can provide routers with information needed for source address validation. This protocol needs to be modified to suit the heterogeneous nature of opportunistic network.

Malicious devices or malicious networks will be able to join an opportunistic network because of the lack of an initial authentication mechanism. Therefore, there is a need to detect and isolate malicious nodes, clusters, or networks. Securely distributing information about malicious

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 81-86 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

entities in the presence of malicious entities is a challenge. If shared securely, this second-hand reputation information can be used by all opportunistic networks nodes to protect themselves from attackers. Even if that information could be distributed securely, avoiding those entities while maintaining connectivity is another challenge.

The solution for the problem of intrusion detection can be referred in [21]. However, we need to emphasize that the highly heterogeneous nature of opportunistic networks makes real-time intrusion detection and response in them even more challenging than in other types of networks.

The intrusion detection approach most relevant for opportunistic networks highlighted in [22], in which autonomous agents perform intrusion detection using embedded detectors. An embedded detector is an internal software sensor that has added logic for detecting conditions that indicate a specific type of attack or intrusion. Embedded detectors are more resistant to tampering or disabling, because they are a part of the program they monitor. Since they are not executing continuously, they impose a very low CPU overhead. They perform direct monitoring because they have access to the internal data of the programs they monitor. Such data does not have to travel through an external path (a log file, for example) between its generation and its use. This reduces the chances that data will be modified before an intrusion detection component gets it.

V. CONCLUSION AND FUTURE SCOPE

The integration of wireless, short-range communication capabilities, with the usage of powerful and smart mobile devices only poised to proliferate; this area of communication possesses innumerable applications like homeland security to Emergency Preparedness Response (EPR), both natural and manmade disaster.

The research in this field can still be considered in its infancy state and can be considered for an introductory material to people who are interested in pursuing research in this field. Opportunistic network applications expose several characteristics and ideas like the exploitation of user's vicinity, user profile-based interest expression, autonomous dissemination of information, an unpredictable communication pattern, and an open and unrelated user group. Current research addresses these ideas or the heterogeneity of the opportunistic network. Most previous research works overlooks the human aspects on opportunistic networks and its applications. So, in this paper we discussed privacy issues and user trust as two crucial human aspects for user's acceptance of opportunistic networks. For both aspects, different research papers in the related fields such as pervasive computing and mobile Ad-hoc network have been surveyed and identified the challenges and suggested the possible solution giving the research the scope to stimulate, model and to implement them. Another aspect is security which a key challenge in open wireless networking environment like the opportunistic network. Some of the security as well as the privacy challenges have been addressed.

The other two important issues which are not discussed are incentive schemes and data forwarding, which can be considered as a very important for the development of the opportunistic network.

Finally two important issues which can be considered are power and memory management. Although current off-the-shelf mobile devices that are suitable for opportunistic network applications, for example PDAs or mobile phones, become more powerful and are equipped with more memory with every new generation, power and memory consumption may remain an issue to solve depending on the application.

REFERENCES

[1] M.Conti L. Pelusi, A.Passarella . "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks." Topics In Ad Hoc And Sensor Networking, IEEE Communications Magazine, 2006.

[2] Naveed Farhana, Nisar Hundewale, "Trust, Privacy and Security in Opportunistic Networks", *2011* 3rd IEEE International Conference on Intelligent Computing and Intelligent Systems (IEEE ICIS 2011) in China.

[3] L. Pelusi, A. Passarella, and M. Conti, "Beyond MANETs:Dissertation on Opportunistic Networking," IIT-CNR Tech. Rep., May 2006.

[4] Satyanarayanan, M. "Pervasive Computing: Vision and Challenges."IEEE Personal Communications 8(4), August, 2001.

[5] H. Liang A. Srinivasan, J. Teitelbaum. "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks." Wiley and Sons.

[6] R. Yahalom, B. Klein, and Delta Th. Beth. "Trust relationships in secure systems- a distributed authentication perspective" In Proceedings, IEEE Symposium on Research in Security and Privacy, pages 150.

[7] Vijay Varadharajan Ching Lin and Yan Wang. "Trust enhanced security for mobile agents. "Seventh IEEE International Conference on E-Commerce Technology,pp .

[8] Andreas Heinemann, Jussi Kangasharju, and Max Muehlhaeuser. "Opportunistic data dissemination using real-world user mobility traces." In AINAW '08: Proceedings of the 22nd International Conference on Advanced Information Networking and Applications - Workshops, pages 1715{1720, Washington, DC, USA, 2008. IEEE Computer Society.

[9] D. Hughes, G. Coulson, and J. Walkerdine. "Free riding on gnutella revisited: the bell tolls? distributed Systems Online, IEEE, 6(6), 2005.

[10] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, no. 8, pp. 102 – 114, Aug 2002.

[11] Y. Chen, W. Xu, W. Trappe, and Y. Zhang, Securing Emerging Wireless Systems: "Lower-layer Approaches." Springer Publishing Company, Incorporated, 2008.

[12] Einar Snekkenes." Concepts for Personal Location Privacy Policies."In Proceedings of the 3rd ACM Conference on Electronic Commerce,pages 48–57. ACM Press, 2001.

[13] Jiejun Kong and Xiaoyan Hong. ANODR: "ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks." In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, pages 291–302. ACM Press, 2003.

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 81-86 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

[14] Hannes Federrath, Anja Jerichow, and Andreas Pfitzmann. "MIXes in Mobile Communication Systems: Location Management with Privacy." In Information Hiding, pages 121–135, 1996.

[15] Alastair R. Beresford and Frank Stajano. "Location Privacy in Pervasive Computing." IEEE Pervasive Computing, 2(1):46–55, 2003.

[16] Marco Gruteser and Dirk Grunwald. "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking." In Proceedings of the First International Conference on Mobile Systems, Applications, and Services (MobiSys), pages 31–42. USENIX, 2003.

[17] L. Lilien, "Opportunistic Sensor Networks," Proposal to the Faculty Research and Creative Activities Support Fund (FRACASF), Western Michigan University, December 2, 2005.

[18] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security & Privacy, Special Issue on Making Wireless Work, Vol. 2(3), May/June 2004, pp.28-39.

[19] C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks," Proc. 8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002), Atlanta, Georgia, September 2002, pp. 12–23.

[20] L. Lilien, Z.H. Kamal, V. Bhuse, and A. Gupta,"Opportunistic Networks: The Concept and Research Challenges in Privacy and Security," Proc. NSF Intl. Workshop of Research Challenges in Security and Privacy for Mobile .

[21] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang. "SAVE: Source Address Validity Enforcement Protocol," UCLA Technical Report 01-0004, Los Angeles, CA, 2001.

[22] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion Detection in Wireless Ad Hoc Networks", IEEE Wireless Communications, Vol. 11(1), February 2004, pp. 48-60.

[23] D. Zamboni, "Using Internal Sensors for Computer Intrusion Detection." CERIAS Technical Report 2001-42, CERIAS, Purdue University, West Lafayette, IN, August 2001.