

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X



IJCSMC, Vol. 4, Issue. 5, May 2015, pg.113 – 116

RESEARCH ARTICLE

P2P CONTENT-BASED FILE SHARING AND PROVIDING SECURITY IN DISCONNECTED MANETS

Ramesh D¹

Student, M.Tech (Computer Networking Engineering), BITM, Bellary, India¹

Pratibha Mishra²

Assistant Professor, Computer Science & Engineering Department, BITM, Bellary, India²

reachramesh2013@yahoo.com, iet_pratibha@yahoo.com

Abstract- In P2P environments, like file sharing methods in mobile ad hoc networks (MANETs) can be classified into three groups: flooding-based, advertisement-based, and social contact-based. The first two groups of methods can easily have high overhead and low scalability. So our concern on third methods adapts to the opportunistic nature of disconnected MANETs, which can be exploited to improve the file searching efficiency. In this project, And by propose a P2P content-based file sharing system, namely SPOON, for disconnected MANETs. It takes advantage of node mobility by designating stable nodes, which have the most frequent contact with community members, as community coordinators for intra community searching, and highly mobile nodes that visit other communities frequently as community ambassadors for intercommunity searching and file sharing. And Additional security issues also be done for the file sharing of information which is transferring in the networks.

Key terms: P2P, MANETs, SPOON

I. INTRODUCTION

Peer-to-Peer networks have been very popular since their first emergence of medical help leads to be done. Some systems have already been deployed to be functional on the Internet. Many peer-to-peer systems currently serve users who are able to share files located at their PCs without requiring information to be used at central servers. Together with the new users of the Internet and the emergence of different types of files to be shared (documents, audio files, etc.), number of users of peer-to-peer systems increases every day (1).

A mobile ad-hoc network is formed dynamically without requiring any wireline infrastructure. Therefore, it has found wide applications in military operations, disaster relief efforts, and more recently, in civilian and ubiquitous environments. In this project, I study a specific type of application: the dissemination of popular data files transfer among the users with disconnected mobile ad hoc network. Such dissemination is peer-to-peer in nature: a mobile node may be a requester of a popular data file, such as an image or an audio clip and it becomes a supplier of this data file after it retrieves the file from other supplier(s). Meanwhile, unlike wired or wireless cellular networks, every mobile node has a limited transmission range. Therefore, two or more mobile nodes can communicate with each other directly, only if they are in the transmission range of each other. To communicate with a peer outside its transmission range, a mobile node has to rely on one or more intermediate peer(s) as relay(s). Due to the free movement of mobile nodes, both direct and indirect connections between peers can be disconnected very frequently (4).

Security is important for these devices to share information. As I deploying prototype wireless network sensors at UC Berkeley. These sensors measure environmental parameters and experimenting with having the control air conditioning and lighting systems. Serious privacy questions arise if third parties can read or tamper with sensor data. In the future, they envision wireless sensor networks being used for emergency and life-critical systems – and here the questions of security are foremost (10).

II. LITERATURE REVIEW

Peer-to-Peer Information Sharing in a Mobile Ad Hoc Environment

Peer to peer file sharing [1] extended the Gnutella system to mobile environments and proposed the use of a set of keywords to represent user interests.

Efficient Content Location in Wireless Ad Hoc Networks

Efficient content location [5] GCLP (Geography-based content location protocol) for efficient content discovery in location-aware ad hoc networks. It disseminates contents and requests in crossed directions to ensure their encountering.

Leveraging Social Networks for P2P Content-Based File Sharing in Mobile Ad Hoc Networks

Leveraging Social Networks [10] the multiple factors (e.g., node mobility, file popularity, and file server topology) in creating file replicas in file servers to realize optimal file availability in content distribution community. In replicas each file to network central locations, which are frequently visited by nodes in the system, to ensure efficient data access between the different mobile nodes in network region.

Socially-Aware Routing for Publish-Subscribe in Delay-Tolerant Mobile Ad Hoc Networks

Social Cast [11] to calculates a node's utility value on an interest based on the node's mobility and co-location with the nodes subscribed to the interest. It public contents on an interest of the user subscribe by forwarding the contents to nodes with the highest utilities on the interest for file sharing and searching.

Secure Aggregation for Wireless Networks

Secure message transfer [6] design is aiming at providing lightweight security mechanisms to effectively detect node misbehavior (dropping, modifying or forging messages, transmitting false aggregate value). An enable a base station to trust results from a sensor network, even if an adversary may be able to deploy intruder nodes inside the network could be shared and recover the key material from a single node. The design exploits two main ideas: delayed aggregation and delayed authentication. Instead of aggregating messages at the immediate next hop, messages are forwarded unchanged over the first hop and then aggregated at the second hop. This increases the transmission costs, but will enable integrity guarantees for networks where two consecutive nodes are not compromised. Instead of attempting to authenticate messages right away, so save resources by authenticating messages after a time delay.

A Socio-Aware Overlay for Publish/Subscribe Communication in Delay Tolerant Networks

Socio-Aware overlay [12] of exploit distributed community detection from the trace and propose a Socio-Aware Overlay over detected communities for publish/subscribe communication. Centrality nodes have the best visibility to the other nodes in the network. Overlay with such centrality nodes from communities. Distributed community detection operates when nodes (i.e. devices) are in contact by gossiping.

III.CONCLUSION

The P2P concept of content-based file sharing through the network shown in system with the secure transfer of data using security factors. So the sharing of information will be secure by the usage of security pair keys to transfer from one node to another until the key matching is done, and then transferred the data. By doing these usually there is no chance of misuse or drop-age of data until the network going to be failed.

REFERENCES

- [1] D.W.A. Hayes, "Peer-to-Peer Information Sharing in a Mobile Ad Hoc Environment," Proc. IEEE Sixth Workshop Mobile Computing Systems and Applications (WMCSA '04), 2004.
- [2] Y. Huang, Y. Gao, K. Nahrstedt, and W. He, "Optimizing File Retrieval in Delay-Tolerant Content Distribution Community," Proc. IEEE 29th Int'l Conf. Distributed Computing Systems (ICDCS '09), 2009.
- [3] M. Papadopoulou and H. Schulzrinne, "A Performance Analysis of 7DS: A Peer-to-Peer Data Dissemination and Prefetching Tool for Mobile Users," Proc. IEEE Sarnoff Symp. Digest Advances in Wired and Wireless Comm., 2006.
- [4] T. Repantis and V. Kalogeraki, "Data Dissemination in Mobile Peer-to-Peer Networks," Proc. Sixth Int'l Conf. Mobile Data Management (MDM '05), 2005.
- [5] J.B. Tchakarov and N.H. Vaidya, "Efficient Content Location in Wireless Ad Hoc Networks," Proc. IEEE Int'l Conf. Mobile Data Management (MDM '04), 2004.
- [6] Lingxuan Hu and David Evans "Secure Aggregation for Wireless Networks" Department of Computer Science University of Virginia Charlottesville, wired and wireless comm., 2009.
- [7] Lei Yu and Jianzhong Li "Secure Continuous Aggregation in Wireless Sensor Networks" Siyao Cheng, Shuguang Xiong, and Haiying Shen, Member, IEEE 2014
- [8] Minos Garofalakis and Joseph M. Hellerstein "Proof Sketches: Verifiable In-Network Aggregation" Petros Maniatis *Intel Research Berkeley* IEEE 2007
- [9] Matthew Baker and Russ Fink "Implementing a Distributed Peer to Peer File Sharing System using CHEWBACCA – CHord, Enhanced With Basic Algorithm Corrections and Concurrent Activation" David Trimm, Adam Whisman IEEE 2003.
- [10] K. Chen and H. Shen, "Leveraging Social Networks for P2P Content-Based File Sharing in Mobile Ad Hoc Networks," Proc. IEEE Eighth Int'l Conf. Mobile Adhoc and Sensor Systems (MASS), 2011.

- [11] P. Costa, C. Mascolo, M. Musolesi, and G.P. Picco, "Socially- Aware Routing for Publish-Subscribe in Delay-Tolerant Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 26, no. 5, pp. 748-760, June 2008.
- [12] E. Yoneki, P. Hui, S. Chan, and J. Crowcroft, "A Socio-Aware Overlay for Publish/Subscribe Communication in Delay Tolerant Networks," Proc. 10th ACM Symp. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM '07), 2007.