Research Journal of Engineering Sciences ISSN 2278 – 9472
Vol. **1(6),** 36-39, December **(2012)** *Res. J. Engineering Sci.*

Review Paper

Routing Protocols in Mobile Ad Hoc Networks

Verma Nupur
Baba Banarasi Das University, Lucknow, UP, INDIA

Available online at: www.isca.in
Received 4th September 2012, revised 15th September 2012, accepted 30th September 2012

Abstract

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links. The design of network protocols for MANETs is a complex issue. These networks need efficient distributed algorithms to determine network organization (connectivity), link scheduling, and routing. An efficient approach is to consider routing algorithms in which network connectivity is determined in the process of establishing routes. Message routing in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as power expended, variable wireless link quality, propagation path loss, fading, multiuser interference, and topological changes, become relevant issues Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange. In addition, mesh-based mobile networks can be operated as robust, inexpensive alternatives or enhancements to cell-based mobile network infrastructures. A MANET protocol should function effectively over a wide range of networking contexts--from small, collaborative, ad hoc groups to larger mobile, multihop network.

Keywords: Protocols, networks, wireless communications technologies.

Introduction

Advances in information technology for these important types of situations are envisioned for future wireless communications. Such network scenarios cannot rely on centralized and organized connectivity, and can be termed as wireless *mobile ad hoc networks* (MANETs). A MANET is an autonomous collection of mobile users (nodes) that communicate over relatively bandwidth-constrained wireless links. Each node is equipped with wireless receivers and transmitters using antennas that may be omni-directional, highly directional, or possibly steerable. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is *decentralized*, where network organization and message delivery must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. Nodes must also contend with the effects of radio communication, including multiuser interference, multipath fading, and shadowing. A MANET may operate in a stand-alone manner, or be connected to a larger network, e.g., the fixed Internet. The design of network protocols for MANETs is a complex issue. These networks need efficient *distributed* algorithms to determine network organization (connectivity), link scheduling, and routing. An efficient approach is to consider routing algorithms in which network connectivity is determined in the process of establishing routes[1]. Message routing in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as power expended, variable wireless link quality, propagation path loss, fading, multiuser interference, and topological changes, become relevant issues. The network should be able to adaptively alter routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks desire to maintain a *low probability of intercept* and/or a *low probability of detection*. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection (or interception). A lapse in any of these requirements may degrade the performance and dependability of the network. Various protocols have been recently proposed in the Internet Engineering Task Force (IETF) for executing routing in a MANET: Zone Routing Protocol (ZRP) \cite{HaaPea97}, Ad Hoc On Demand Distance Vector (AODV) Routing \cite{PerRoy98}, Temporally-Ordered Routing Algorithm (TORA) \cite{ParCor98}, Dynamic Source Routing (DSR) Protocol \cite{BroJohMal98}, Cluster Based

Routing Protocol (CBRP) \cite{JiaLiTay98}, Ad Hoc Multicast Routing Protocol (AMRoute) \cite{BomMcaTalLiu98}, Core Extraction Distributed Ad Hoc Routing (CEDAR) \cite{SivSinBha98}, On-Demand Multicast Routing Protocol (ODMRP) \cite{GerPeiLeeChi98}, and Optimized Link State Routing Protocol (OLSRP) \cite{JacMuhQay98}. Other projects are being pursued for mobile wireless networks, such as the Wireless Internet Gateways (WINGS) project \cite{GarFulMadBeyFri97} and the Multimedia Support for Mobile Wireless Networks (MMWN) \cite{RamSte97} and Density and Asymmetry Adaptive Network (DAWN) projects for DARPA's Global Mobile Information Systems (GloMo) program. While these protocols are not designed specifically for MANETs, they may provide enhanced performance and robustness over the proposed MANET routing protocols[2]. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. It is unlikely that a single routing protocol will be optimal for all scenarios. A given protocol will execute efficiently in those networks whose characteristics are in accord with the mechanisms used by the protocol. However, any protocol must efficiently handle several inherent characteristics of MANETs:

Dynamic topology: Mobility of nodes lends to unpredictable network topology.

Variable capacity wireless links: Wireless links are bandwidth-constrained. Moreover, since wireless links have lower capacity than hardwired links, traffic congestion is typical rather than atypical. However, as a MANET is often an extension of a fixed network, the same services and demands must be accommodated. These demands will increase as multimedia computing and networking become more mainstream.

Power constrained operation: Power conservation is *crucial* in mobile wireless systems since these networks typically operate off power-limited sources, which dictate whether a network is operational or not.

Physical security: Mobile networks are more vulnerable to physical security threats such as eavesdropping and jamming attacks. The merit of a routing protocol is judged with performance metrics, both qualitative and quantitative. Desirable *qualitative* properties of a MANET routing protocol include the following:

Distributed: The decentralized nature of a MANET requires that any routing protocol execute in a distributed fashion.

On demand operation: Since a uniform traffic distribution can not be assumed within the network, the routing algorithm must adapt to the traffic pattern on a demand or need basis, thereby utilizing power and bandwidth sources more efficiently.

Loop-free: To ensure proper message delivery and efficient network operation, a routing protocol must be loop-free.

Security: Since MANETs are more vulnerable to physical security threats, provisions for security must be made, e.g., the application of Internet Protocol (IP) security techniques.

Entering/Departing nodes: A ting protocol should be able to quickly adapt to entering or departing nodes in the network, without having to restructure the entire network.

Bidirectional/Unidirectional links: Since the condition of a MANET is dynamic, a routing to col should be able to execute on both bidirectional and unidirectional links. In this paper, we develop a dynamic power-conscious uting algorithm that incorporates physical layer and link layer statistics. This algorithm Routing decisions are made based on feedback or information extracted from the received signal. In this paper, we identify and define meaningful trics for assessing the performance of MANET protocols[3]. We design and build a unified simulation and update the performance of the different protocols proposed in the IETF in different scenarios. Moreover, we idenentify critical features required for military MANETs and evaluate the protocols in this context.

Applications

The technology of Mobile Ad hoc Networking is somewhat synonymous with Mobile Packet Radio Networking (a term coined via during early military research in the 70's and 80's), Mobile Mesh Networking (a term that eared in an article in The Economist regarding the structure of future military networks) and Mobile, Multihop, Wireless Networking (perhaps the most accurate term, although a bit cumbersome)[4].

There is current and future need for dynamic ad hoc networking technology. The emerging field of mobile and nomadic computing, with its current emphasis on mobile IP operation, should gradually broaden and require highly-adaptive mobile networking technology to effectively manage multihop, ad hoc network clusters which can operate autonomously or, more than likely, be attached at some point(s) to the fixed Internet. Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange. In addition, mesh-based mobile networks can be operated as robust, inexpensive alternatives or enhancements to cell-based mobile network infrastructures. There are also existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks[5] many of these networks consist of highly-dynamic autonomous topology segments. Also, the developing technologies of "wearable" computing and communications may provide applications for MANET technology. When properly combined with satellite-based information delivery, MANET technology can provide an extremely flexible method for establishing communications for

fire/safety/rescue operations or other scenarios requiring rapidly-deployable communications with survivable, efficient dynamic networking. There are likely other applications for MANET technology which are not presently realized or envisioned by the authors. It is, simply put, improved IP-based networking technology for dynamic, autonomous wireless networks.

Characteristics of MANETs

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internetwork. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omnidirectional (broadcast), highly-directional (point-to-point), possibly steerable, or some combination thereof[6]. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

MANET Routing Protocol Performance Issues

To judge the merit of a routing protocol, one needs metrics—both qualitative and quantitative--with which to measure its suitability and performance. These metrics should be *independent* of any given routing protocol.

The following is a list of desirable qualitative properties of MANET routing protocols: i. Distributed operation: This is an essential property, but it should be stated nonetheless. ii. Loop-freedom: Not required per se in light of certain quantitative measures (i.e. performance criteria), but generally desirable to avoid problems such as worst-case phenomena, e.g. a small fraction of packets spinning around in the network for arbitrary time periods. Ad hoc solutions such as TTL values can bound the problem, but a more structured and well-formed approach is generally desirable as it usually leads to better overall performance.

A MANET protocol should function effectively over a wide range of networking contexts--from small, collaborative, ad hoc groups to larger mobile, multihop networks[7]. The discussion of characteristics and evaluation metrics somewhat differentiate MANETs from traditional, hardwired, multihop networks. The wireless networking environment is one of scarcity rather than abundance, wherein bandwidth is relatively limited, and energy may be as well. The networking opportunities for MANETs are intriguing and the engineering tradeoffs are many and challenging. A diverse set of performance issues requires new protocols for network control. (In Proceedings of the *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),* San Antonio, TX, January 27-31, 2002)

Secure Routing for Mobile Ad hoc Networks

The emergence of the Mobile Ad Hoc Networking (*MANET*) technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks[8]. In either case, the proliferation of *MANET*-based applications depends on a multitude of factors, with trustworthiness being one of the primary challenges to be met. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In particular, in *MANET*, any node may compromise the routing protocol functionality by disrupting the route discovery process[9]. In this paper, we present a route discovery protocol that mitigates the detrimental effects of such malicious behavior, as to provide correct connectivity information. Our protocol guarantees that fabricated, compromised, or replayed route replies would either be rejected or never reach back the querying node. Furthermore, the protocol responsiveness is safeguarded under different types of attacks that exploit the routing protocol itself[10]. The sole requirement of the proposed scheme is the existence of a security association between the node initiating the query and the sought destination. Specifically, no assumption is made regarding the intermediate nodes, which may exhibit arbitrary and malicious behavior. The scheme is robust in the presence of a number of non-colluding nodes, and provides accurate routing information in a timely manner.

Conclusion

It is concluded that MANET is one of the popular adhoc network and feasible wireless technology as well as advanced mobile computing which has envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies. They are composed of relatively bandwidth-constrained wireless links. The design of network protocols for MANETs is a complex issue. These networks need efficient distributed algorithms to determine network organization (connectivity), link scheduling, and routing. An efficient approach is to

consider routing algorithms in which network connectivity is determined in the process of establishing routes. Message routing in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. A MANET protocol should function effectively over a wide range of networking contexts--from small, collaborative, ad hoc groups to larger mobile, multihop network.

References

1. Papadimitratos P. and Haas Z.J., Secure Message Transmission in Mobile Ad Hoc Networks, submitted for publication

2. Papadimitratos P., Secure Routing: Methods for Protecting Routing Infrastructures–A Survey, work in progress. JUNE

3. Lamport L., Shostak R. and Pease M., The Byzantine Generals Problem, ACM Trans. Program, Languages, **4(3)**, 382-401 **(1982)**

4. Stajano F. and Anderson R., The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks, Security Protocols, 7th International Workshop, LNCS, Springer-Verlag **(1999)**

5. Zhou L. and Haas Z.J., Securing Ad Hoc Networks, IEEE Network Magazine, **13(6)**, **(2009)**

6. IEEE Std. 802.11, Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications **(1999)**

7. Zucceratto R. and Adams C., Using Elliptic Curve Diffie-Hellman in the SPKM GSS-API, Internet Draft, IETF, Aug. **(1999)**

8. Johnson D.B. et al, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, Internet Draft, IETF MANET Working Group, March 2nd **(2011)**

9. Krawczyk H., Bellare M. and Canetti R., HMAC Keyed-Hashing for Message Authentication, RFC 2104, February **(1997)**

10. Adamson B., Tactical Radio Frequency Communication Requirements for IPng, RFC 1677, **(2011)**

11. Madhavi W. Subbarao, Performance of Routing Protocols for Mobile Ad-Hoc Networks 2011-12, Panagiotis Papadimitratos and Zygmunt J. Haas Wireless Networks Laboratory **(2012)**