Research Journal of Computer and Information Technology Sciences
Vol. **1(1),** 14-17, February **(2013)** *Res. J. Computer & IT Sci.*

Review Paper

Security and Energy efficiency in Ad Hoc Networks

Lakshmi P.S. [1], Pasha Sajid[2] and Ramana M.V.[3]
[1,2]Swarna Bharathi Institute of Science and Technology, Khammam, AP, INDIA
[3]SR & BGNR Govt. Arts & Science College, Khammam, AP, INDIA

Available online at: www.isca.in
Received 7th Dcember 2012, revised 31st December 2013, accepted 18th January 2013

Abstract

Many wireless networking problems have to be solved for the efficient design and deployment of the communication devices that operate in a Mobile AdHoc Network (MANET) environment. An AdHoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. Due to number of constraints in self-organizing and self-operating networks, routing of it is a challenging problem. A performance evaluation of routing protocol is very cumbersome due to various metrics involving dynamic topologies, mobility, routing limited resources, security etc. To find the optimum routes with minimum control overhead and network resources, there are a lot of routing-protocols namely DSDV, DSR, AODV, TORA, etc. In this paper security and energy efficient routing algorithms for MANETs are surveyed, categorized and analyzed, highlighting their strengths and weaknesses.

Keywords: Security, Energy efficiency, wireless networking problems, mobile AdHoc network.

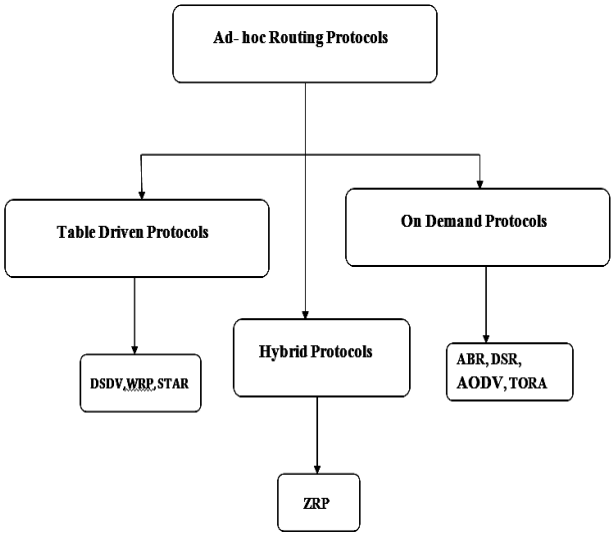
Introduction

The Internet Engineering Task Force has defined a Mobile Adhoc Network (MANET) as: "An autonomous system of mobile routers (and associated hosts) connected by wireless links--the union of which form an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet".

The Mobile Adhoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. Under these circumstances, routing is much more complex than in conventional (static) networks. Many of the possible solutions are determined by the characteristics of the media, the behavior of nodes and the data flow. For a successful deployment, this is an important problem, since a wrong choice may have a severe impact on the performance, and consequently on the acceptance of the new technology. Also, providing just any protocol is not feasible, due to the different requirements on hardware and lower network layers.

This paper is organized as follows: Section 2 presents a brief description of need of routing protocols and their classification. Section 3 describes the routing protocols like AODV, TORA, DSR and DSDV. Section 4 focuses on security goals and energy efficient protocol in MANETs. Section 5 is dedicated to the future scope and Section 6 provides conclusions.

Need of routing protocols: To find an efficient route for an un-interrupted communication, many protocols are suggested keeping applications and type of network in view. The main problem with ad-hoc networking is how to send a message from one node to another with no direct link. The nodes in the network are moving around unpredictably, and it is very challenging which nodes that are directly linked together. The topology of an ad-hoc network is constantly changing and it is very difficult for routing process[1]. There are two main approaches for routing process in ad hoc networks. The first approach is a proactive approach which is table driven and uses periodic protocol



Classification of Routing Protocols: The routing protocols can be classified into two parts: i. Table driven and ii. Source initiated (on demand) while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing[2]. Flat routing covers both routing protocols based on routing strategy. The three ad hoc routing protocols are used, AODV, DSDV and DSR. AODV and DSR is Reactive (On demand) whereas DSDV is Proactive (Table driven) Routing protocol.

Proactive or Table-Driven Routing Protocols: The proactive routing protocols are table-driven[3]. They usually use link-state Routing algorithms flooding the link information. Link-state algorithms maintain a full or partial copy of the network topology and costs for all known links. Thus, link-state routing algorithms are more reliable, less bandwidth-intensive, but also more complex and compute- and memory-intensive. These are called table driven protocols. In these protocols, each node maintains routing information to every other node in the network. The routing information is usually kept in number of different routing tables. These tables are periodically updated if the network topology changes. The difference between these protocols exists in the way the routing information is updated, detected and type of information kept at each routing. Some of the most used on proactive routing protocols are DSDV [4] and WRP[4].

Reactive or On Demand Routing Protocol: In Reactive routing protocols, when a source wants to send packets to a destination, it invokes the route discovery mechanisms to find the route to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. Unlike table driven protocols, all nodes need not maintain up-to-date routing information. Some of the most used on demand routing protocols are DSR [5] and AODV [6].

Hybrid Routing Protocol: Hybrid routing protocol combines the advantages of both proactive and reactive routing protocols. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. Some of the existing hybrid protocols are ZRP[5].

Description of Selected Routing Protocols

Adhoc On-demand Distance Vector routing protocol – AODV: The Ad-hoc On-demand Distance Vector routing protocol[7,8] enables multi-hop routing between the participating mobile nodes wishing to establish and maintain an ad-hoc network. AODV is a reactive protocol based upon the distance vector algorithm. The algorithm uses different messages to discover and maintain links. Whenever a node wants to try and find a route to another node it broadcasts a Route Request (RREQ) to all its neighbors. The RREQ propagates through the network until it reaches the destination or the node with a fresh enough route to the destination. Then the route is made available by uncasing a RREP back to the source.

The algorithm uses hello messages (a special RREP) that are broadcasted periodically to the immediate neighbors. These hello messages are local advertisements for the continued presence of the node, and neighbors using routes through the broadcasting node will continue to mark the routes as valid[9]. If hello messages stop coming from a particular node, the neighbor can assume that the node has moved away and mark that link to the node as broken and notify the affected set of nodes by sending a link failure notification (a special RREP) to that set of nodes.

Temporally - Ordered Routing Algorithm – TORA: TORA protocol[10] belongs to the class of reactive protocols. The protocol is highly adaptive, efficient and it is used to establish the "temporal order" of topological change events which is used to structure the reaction to topological changes. The protocol is designed to minimize reaction to topological changes. The protocol is distributed in that nodes need only maintain information about adjacent nodes. The protocol is "source initiated" and quickly creates a set of routes to a given destination only when desired. The protocol accomplishes three functions through the use of three distinct control packets[11] such as query (QRY), update (UPD) and clear (CLR). QRY packets are used for both creating and maintaining routes, and CLR packets are used for erasing routes[12].

Dynamic Source Routing-DSR: Dynamic Source Routing (DSR)[13] belongs to the class of reactive protocols and allows to dynamically discovering a route across multiple network hops to any destination. Source routing means that each packet in its header carries the complete ordered list of nodes through which the packet must pass. DSR uses no periodic routing of messages, thereby reducing network bandwidth overhead, conserving battery power and avoiding large routing updates throughout the ad-hoc network. Instead DSR relies on support from the MAC layer [11].

In general, systems are designed for the worst-case propagation conditions; however, because of the unpredictability of radio channels, a system can also be designed to adapt to the link quality at both the link layer and the network layer level.

Destination-Sequenced Distance Vector protocol –DSDV: DSDV is well known table driven protocol, based on Bellman-Ford routing mechanism. Freedom from loops in routing table is the key aspect of this protocol. Some other characteristics are more dynamic and less convergence time[14]. Each node maintains a routing table which contains a list of all possible destination nodes within the network along with the no. of hops required to reach to particular node[14]. Each entry of the table marked with a sequence number assigned by the destination node which identifies stale routes, thus avoids formation of loops[15-17]. Every node keep a route table <Destination-address,

Metric, Sequence-no.> for every possible destination. It is non-scalable.

Security Goals

To secure the routing protocols in MANETs, researchers have considered the following security services: availability, confidentiality, integrity, authentication and non-repudiation[18-20]. Availability guarantees the survivability of the network services despite attacks. A Denial-of-Service (DoS) is a potential threat at any layer of an ad hoc network. On the media access control layer, an adversary could jam the physical communication channels. On the network layer disruption of the routing operation may result in a partition of the network, rendering certain nodes inaccessible. On higher levels, an attacker could bring down high-level services like key management service.

Confidentiality ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications. Routing information must also remain confidential in some cases, because the information might be valuable for enemies to locate their targets in a battlefield.

Integrity ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information. Non-repudiation ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

The networking environment in wireless schemes makes the routing protocols vulnerable to attacks ranging from passive eavesdropping to active attacks such as impersonation, message replay, message littering, network partitioning, etc. Eavesdropping is a threat to confidentiality and active attacks are threats to availability, integrity, authentication and non-repudiation. Nodes roaming in an ad hoc environment with poor physical protection are quite vulnerable and they may be compromised. Once the nodes are compromised, they can be used as starting points to launch attacks against the routing protocols.

Energy Efficient Routing Protocol in MANETs: The network lifetime[21] is a key design factor of mobile ad hoc networks (MANETs). To prolong the lifetime of MANETs, one is forced to attain the tradeoff of minimizing the energy consumption and load balancing. In MANETs, energy waste resulting from retransmission due to high frame error rate (FER) of wireless channel is significant. In this paper, we propose a novel protocol termed error-aware candidate set routing protocol (ECSRP). ECSRP chooses a route in a candidate subset in the route cache in which all the nodes have enough residual battery power. This approach avoids overusing certain routes. If multiple routes exist in the candidate set, ECSRP employs a metric achieving the tradeoff between energy-efficiency and load balancing to select the optimal route. It also takes channel condition into consideration by incorporating packet loss probability in the computation of energy consumption. This helps to reduce the number of retransmissions and save energy.

PUMA: PUMA (Protocol for Unified Multicasting through Announcement) does not require any unicast routing protocol to operate, or the pre-assignment of cores to groups. The section below shows PUMA operation in detail. PUMA derives from its use of very simple signaling (multicast announcements) to accomplish all the functions needed in the creation and maintenance of a multicast routing structure in a MANET[23,24]. Multicast announcements are used to elect cores dynamically, determine the routes for sources outside a multicast group to unicast multicast data packets towards the group, join and leave the mesh of a group, and maintain the mesh of the group. PUMA protocol is advantageous due to its high packet delivery ratio and limited congestion.

PUMA provides the lowest and a very tight bound for the control overhead compared to ODMRP and MAODV. In other words, the control overhead of PUMA is almost constant node when mobility, number of senders, multicast group size or traffic load is changed. It also provides the highest packet delivery ratio for all scenarios. The mesh constructed by PUMA provides redundancy to the region containing receivers, thus reducing unnecessary transmissions of multicast data packets. PUMA does not depend on the existence of any specific pre-assigned unicast protocol.

Future scope

There is a scope to mainly focus on performance analysis of PUMA and to achieve secure PUMA in Ad hoc network. There is a strong to focus on the need to have a secure multicasting after more analysis on key management schemes.

Conclusion

This paper presents a survey on various routing protocols in MANETs based on security and energy efficiency. To improve efficiency, it is essential to model the performance of existing protocols. In order to do so, we have compared the performance of Proactive (TBRPF) and Reactive (ADOV and DSR) routing protocols for mobile ad hoc networks in terms of Throughput and End to End Delay.

References

1. Mahdavi J., PSC, Floyd S., LBNL, Romanow A., Sun Microsystems, TCP Selective Acknowledgment Options, IETF RFC 2018, October **(1996)**

2. Kapang Lego, Pranav Kumar, Dipankar Sutradhar Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Ad hoc Network Kapang Lego et. *All Indian Journal of Computer Science and Engineering,* **1(4),** 364-371 **(2001)**

3. George Sklyarenko, AODV Routing Protocol, Seminar Technische Informatik, Institute for Informatik, Freie University at Berlin, Takustr. 9, D-14195, Berlinm, Germany, July **(2006)**

4. Kuppusamy P., Thirunavukkarasu K., Kalaavathi B., A Study and Comparison of OLSR, AODV and TORA Routing Protocols in Ad Hoc Networks, *IEEE* **(2011)**

5. Shaily Mittal1, Prabhjot Kaur, PERFORMANCE COMPARISION OF AODV, DSR and ZRP ROUTING PROTOCOLS IN MANET'S, 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, DOI 10.1109 , IEEE **(2009)**

6. Krishna Gorantala, Routing Protocols in Mobile Ad-hoc Networks, Umea University Department of Computing Science SE-901 87 UMEA SWEDEN **(2006)**

7. Holland H. and Vaidya N.H, Analysis of TCP performance over mobile ad-hoc networks, in Proceedings of IEEE/ACM Mobicom99, pages 219-230, Seattle, WA, USA, August **(1999)**

8. Operational Requirements Document (ORD) for Joint Tactical Radio System (JTRS), JTRS Joint Program Office, 23 March **(1998)**

9. Theriot Ty, Simulation and Performance Analysis of the AODV protocol for Tactical Mobile Ad-hoc Networks, Master's Thesis, Naval Postgraduate School, Monterey, California, December **(2000)**

10. Vaidya Nitin H., Mobile Ad Hoc Networks; Routing, MAC, and Transport Issues, MobiComm Tutorial, 1- 431 **(2000)**

11. IEEE, IEEE std 802.11 - wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 16 November **(1997)**

12. Postel J., ISI, User Datagram Protocol, IETF RFC 768, August **(1980)**

13. Xu S., Saadaei T., Does the IEEE 802.11MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?, in *IEEE Communications Magazine,* **39(6),** 130-137 **(2001)**

14. Khaleel Ur Rahman Khan, A Venugopal Reddy, Rafi U. Zaman, K. Aditya Reddy, T. Sri harsha, An Efficient DSDV Routing Protocol for Wireless Mobile Adhoc Networks and its Performance Comparison Second UKSIM European Symposium on Computer Modeling and Simulation **(2008)**

15. Sunil Taneja, Ashwani Kush, A Survey Of Routing Protocols in Mobile Ad Hoc Networks International Journal of Innovation, Management and Technology, **1(3),** ISSN:2010-0248 **(2010)**

16. Arun Kumar B.R., Lokanatha C.Reddy, Prakash S. Hiremath, Performance Comparision of Wireless Mobile ad Hoc Network Routing Protocols IJCSNS *International Journal of Computer Science And Network Security,* **8(6) (2008)**

17. Mbarushimana C. and Shahrabi A., Comparative Study of Reactive and proactive Routing Protocols Performance in Mobile Ad Hoc Networks, Proc. of The 21st International conference on Advanced Information Networking and Applications Workshops (AINAW'07), 679-684 **(2007)**

18. Mishra Amitabh, Nadkarni Ketan M. and Ilyas Mohammad. Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network, CRC PRESS Publisher **(2003)**

19. Siva Ram C. Murthy and Manoj B.S., Ad hoc wireless networks: Architecture and Protocols, Prentice Hall Publishers, ISBN 013147023X **(2004)**

20. William Stallings, Network Security essentials: Application and Standards, Pearson Education, Inc, ISBN 0130351288 **(2003)**

21. An Error-aware and Energy Efficient Routing Protocol in MANETs Liansheng Tan; Peng Yang; Chan,S. Computer Communications and Networks, 2007, ICCCN **(2007)**

22. Power Management Based Grid Routing Protocol for IEEE 802.11 Based MANET: Li Xu and Bao-yu Zheng , Grid and Co-operative computing GCC, **3254,** 753-760 **(2004)**

23. Dewan Tanvir Ahmed Multicasting in Ad Hoc Networks University of Ottawa dahmed@site.uottawa.caCSI5140F Wireless Ad Hoc Networking Professor Ivan Stojmenovic Ottawa, Ontario, Canada, Fall **(2005)**

24. Cheng M., Shun J., Min M., Li Y. and Wu W., Energy-Efficient Broadcast and Multicast Routing in Multihop Ad Hoc Wireless Networks, Wireless Communications and Mobile Computing, **6(2),** 213–223 **(2006)**