A Review on Mobile Ad-Hoc Networks (MANET) Routing Protocols

Gurinder Pal Singh Chakkal[1], Sukhdeep Singh Dhillon[2]
Computer Science & Engineering [1, 2]
Institute of Engineering & Technology Bhaddal, Ropar

Abstract
The increase in availability and popularity of mobile wireless devices has lead researchers to develop a wide variety of Mobile Ad-hoc Networking (MANET) protocols to exploit the unique communication opportunities presented by these devices. Devices are able to communicate directly using the wireless spectrum in a peer-to-peer fashion, and route messages through intermediate nodes, however the nature of wireless shared communication and mobile devices result in many routing and security challenges which must be addressed before deploying a MANET. In this paper we investigate the range of MANET routing protocols available and discuss the functionalities of several ranging from early protocols such as DSDV to more advanced such as MAODV, our protocol study focuses upon works by Perkins in developing and improving MANET routing. A range of literature relating to the field of MANET routing was identified and reviewed, we also reviewed literature on the topic of securing AODV based MANETs as this may be the most popular MANET protocol. The literature review identified a number of trends within research papers such as exclusive use of the random waypoint mobility model, excluding key metrics from simulation results and not comparing protocol performance against available alternatives.

Key words: Aodv, Manet, Routing Protocols.

1. INTRODUCTION

Wireless technologies such as Bluetooth or the 802.11 standards enable mobile devices to establish a Mobile Ad-hoc Network (MANET) by connecting dynamically through the wireless medium without any centralized structure [1]. MANETs offer several advantages over traditional networks including reduced infrastructure costs, ease of establishment and fault tolerance, as routing is performed individually by nodes using other intermediate network nodes to forward packets [2], this multi-hopping reduces the chance of bottlenecks, however the key MANET attraction is greater mobility compared with wired solutions.

There are a number of issues which affect the reliability of Ad-hoc networks and limit their viability for different scenarios; lack of centralized structure within MANET requires that each individual node must act as a router and is responsible for performing packet routing tasks; this is done using one or more common routing protocols across the MANET [3]. Performing routing tasks requires memory and computation power, however mobile devices feature physical size and weight limitations essential for their mobility, this reduces the available memory and computational resources as well as limiting battery power.

MANETs containing more nodes require greater processing power, memory and bandwidth to maintain accurate routing information; this introduces traffic overhead into the network as nodes communicate routing information, this in turn uses more battery power**.**Wireless technologies

use a shared communication medium; this causes interference which degrades network performance when multiple nodes attempt to transmit simultaneously. Techniques such as Distributed Coordination Function (DCF) are used to limit the impact of channel contention upon network performance, DCF uses carrier sense multiple access with collision avoidance (CSMA/CA) and channel switching to reduce interference [4] however larger MANETs feature more interference. The mobility of nodes is also a major factor within MANETs due to limited wireless transmission range; this can cause the network topology to change unpredictably as nodes enter and leave the network [5]. Node mobility can cause broken routing links which force nodes to recalculate their routing information; this consumes processing time, memory, device power and generates traffic backlogs and additional overhead traffic on the network [6].
Security of MANETs is another major deployment concern; due to the mobility and wireless nature of the network malicious nodes can enter the network at any time, the security of the nodes and the data transmitted needs to be considered [7].Due to these issues ad-hoc networks are not appropriate for most general usage of mobile devices, where internet access is the key requirement; in these situations wireless devices typically connect into the wired infrastructures through access points (AP) to reduce the unreliability of the wireless domain [8].Restructure is not available; including disaster or military scenarios or in low power wireless sensor networks or vehicles which only need to communicate with each other [9].
This paper is structured as follows; Section II discusses the core requirements of a MANET routing protocol, Section III discusses MANET routing principles, Section IV investigates some of the earliest MANET routing protocols; DSR and DSDV as well as the impact of mobility models on simulations. Section V focuses upon the AODV MANET routing protocol, Section VI highlights improvements made to AODV in the form of multicasting, section VII investigates security systems designed to AODV and Section VIII concludes the paper and proposes future work.

2. LITERATURE REVIEW

We have identified several pieces of key literature in the field of MANET routing protocols which highlight existing protocols as well as the current thinking within the field and the directions researchers are moving in the future. Reference [3] proposes that an effective MANET routing protocol must be equipped to deal with the dynamic and unpredictable topology changes associated with mobile nodes, whilst also being aware of the limited wireless bandwidth and device power considerations which may lead to reductions in transmission range or throughput. This is expanded upon by [1] who propose that in addition to these core requirements; MANET routing protocols should also be decentralized, self-healing and self-organizing and able to exploit multi-hopping and load balancing, these requirements ensure MANET routing protocols ability to operate autonomously.

3. MANET ROUTING PRINCIPLES

The first pieces of literature we will discuss are a pair of survey papers by [1], [8], these two survey papers gather together information on the wide variety of MANET routing protocols which researchers have developed to meet the challenges of MANET routing, many of which feature different methods of managing the issues associated with mobility.
Reference [8] performed an extensive research survey into the available routing protocols and attempted to categories them by the features they exhibit and provide details on the core

protocols of each category. This is similar to work undertaken by [1] who took a similar approach in grouping routing protocols using the categories; geographical, multi-path, hierarchical, geo-cast and power aware routing protocols. The two survey papers both find that every protocol identified also fit into the core categories of; reactive, proactive or hybrid routing protocols in additional to any other characteristics they exhibit.

3.1 Proactive Routing

Proactive protocols rely upon maintaining routing tables of known destinations, this reduces the amount of control traffic overhead that proactive routing generates because packets are forwarded immediately using known routes, however routing tables must be kept up-to-date; this uses memory and nodes periodically send update messages to neighbors, even when no traffic is present, wasting bandwidth [10]. Proactive routing is unsuitable for highly dynamic networks because routing tables must be updated with each topology change, this leads to increased control message overheads which can degrade network performance at high loads [11].

3.2 Reactive Routing

Reactive Protocols use a route discovery process to flood the network with route query requests when a packet needs to be routed using source routing or distance vector routing. Source routing uses data packet headers containing routing information meaning nodes don't need routing tables; however this has high network overhead. Distance vector routing uses next hop and destination addresses to route packets, this requires nodes to store active routes information until no longer required or an active route timeout occurs, this prevents stale routes [10]. Flooding is a reliable method of disseminating information over the network, however it uses bandwidth and creates network overhead, reactive routing broadcasts routing requests whenever a packet needs routing, this can cause delays in packet transmission as routes are calculated, but features very little control traffic overhead and has typically lower memory usage than proactive alternatives, this increases the scalability of the protocol [1].

3.3 Hybrid Routing

Hybrid protocols combine features from both reactive and proactive routing protocols, typically attempting to exploit the reduced control traffic overhead from proactive systems whilst reducing the route discovery delays of reactive systems by maintaining some form of routing table [10].The two survey papers [1], [8] successfully collect information from a wide range of literature and provide detailed and extensive reference material for attempting to deploy a MANET, both papers reach the conclusion that no single MANET routing protocol is best for every situation meaning analysis of the network and environmental requirements is essential for selecting an effective protocol. Whilst these papers contain functionality details for many of the protocols available, performance information for the different protocols is very limited and no details of any testing methodologies is provided, because of this the validity of some claims made cannot be verified.

3.4 EARLY MANET ROUTING PROTOCOLS

The next piece of literature is a protocol performance comparison by [12] which compares the proactive Destination Sequenced Distance Vector (DSDV) protocol and the reactive Dynamic Source Routing (DSR) protocol; these protocols were developed in 1994 and were amongst the earliest MANET routing protocols identified using the previous survey papers.

3.4.1 Destination Sequenced Distance Vector (DSDV)

The proactive DSDV protocol was proposed by [13] and is based upon the Bellman-Ford

algorithm to calculate the shortest number of hops to the destination [11]. Each DSDV node maintains a routing table which stores; destinations, next hop addresses and number of hops as well as sequence numbers; routing table updates are sent periodically as incremental dumps limited to a size of 1 packet containing only new information [12].

DSDV compensates for mobility using sequence numbers and routing table updates, if a route update with a higher sequence number is received it will replace the existing route thereby reducing the chance of routing loops, when a major topology change is detected a full routing table dump will be performed,

3.4.2 Dynamic Source Routing (DSR)

The reactive DSR Protocol was developed by [14], operation of the DSR protocol is broken into two stages; route discovery phase and route maintenance phase, these phases are triggered on demand when a packet needs routing. Route discovery phase floods the network with route requests if a suitable route is not available in the route [12].

DSR uses a source routing strategy to generate a complete route to the destination, this will then be stored temporarily in nodes route cache [15]. DSR addresses mobility issues through the use of packet acknowledgements; failure to receive an acknowledgement causes packets to be buffered and route error messages to be sent to all upstream nodes. Route error messages trigger the route maintenance phase which removes incorrect routes from the route cache and undertakes a new route discovery phase [14].

3.4.3 Mobility Models

Reference [12] compares the performance of DSR and DSDV using simulations against 4 different mobility models; these are mathematic models which control the motion of nodes around the simulation; this allows researchers to measure the effect of mobility upon the routing protocols performance. Various mobility models are used to simulate different situations such as high speed vehicular networks or lower mobility ad-hoc conference users, however research by [15] reveals that many studies perform protocol evaluation almost exclusively using the random waypoint mobility model. This research is supported by findings from [2] who claim that the random waypoint model is the most widely used mobility model, however discrepancies were identified between the models behavior and real world scenarios where users typically move in groups, due to this the model may not be appropriate for exclusive testing.

Reference [12] performs simulations against multiple mobility models using networks of varying sizes up to 100 nodes; this increases the accuracy and reliability of the data and reveals network performance under different conditions, the study revealed that DSR gave greater network throughput than DSDV in all tests. These findings cannot be considered conclusive evidence of DSRs superiority because the study only collected network throughput metrics; this information alone does not give an accurate representation of the network performance; collection of other metrics such as packet delivery ratio or end-to-end delay should be considered as these are important metrics for evaluating performance.

3.4.4 SECOND GENERATION MANET ROUTING PROTOCOL –AODV

Researchers learned many lessons from early MANET protocols such as DSR and DSDV, these lead to proposals for new protocols to improve performance, one of the most significant contributions to MANET routing was the Ad-hoc On-demand Distance Vector (AODV) protocol which was designed by [16] as an improvement upon previous work on the DSDV protocol with [13]. Reference [17] has produced a paper discussing the protocols functionality and testing it

against a number of criteria.

3.4.5 Ad-Hoc on-Demand Distance Vector (AODV)

AODV utilizes sequence numbers and routing beacons from DSDV but performs route discovery using on-demand route requests (RREQ); the same process as the DSR protocol [17]. AODV is different to DSR in that it uses distance vector routing; this requires every node in the route to maintain a temporary routing table for the duration of the communication. AODV has improved upon the DSR route request process using an expanding ring search mechanism based upon incrementing time-to-live (TTL) to prevent excessive RREQ flooding [2]. Nodes within an active route record the senders address, sequence numbers and source / destination IP address within their routing tables, this information is used by route reply (RREP) to construct reverse paths [11].

AODV deals with node mobility using sequence numbers to identify and discard outdated routes, this is combined with route error (RERR) messages which are sent when broken links are detected, RERR packets travel upstream to the source informing nodes to delete the broken links and trigger new route discovery if alternative routes are not available [4].

Reference [17] discusses the core principles of the protocol but provide no real insight into possible directions the protocol could take in the future, the network simulation collects data on a number of important metrics; dropped packets, transmission and receiving throughput (UDP and TCP), delay, send time vs. delay, jitter and round trip time. These metrics are all important for quality of service considerations and useful indicators of network performance, however the simulations are run only using AODV protocol so no direct comparison between alternative protocols can be made, the simulation topology also uses a uniform random waypoint mobility model of 16 nodes which as discussed previously in Section IV. C is not an ideal testing environment.

Architecture as the AODV protocol with some modifications and the addition of Multicast Activations (MACT) and Group Hello (GRPH) messages, each node also maintains separate unicast and multicast routing tables [20]. When MAODV broadcasts RREQ messages onto the network they now support multiple destination IP addresses, each of these IP addresses will reply with RREP packets as per AODV behavior however upon receipt of a RREP packet the source will send a MACT to the destination node activating a multicast route. Multicast paths are added to a multicast delivery tree which is stored on the source; this tree records all multicast destinations and allows the node to learn unicast destinations from the tree without broadcasting RREQ [18]. The first node to join a multicast group becomes the leader of that group responsible for group maintenance; this is done using by broadcasting GRPH messages which contain the leaders IP, these GRPH messages are used to synchronize the multicast group using incrementing sequence numbers [19]. Should a tree group member become disconnected it will attempt to reconnect to the existing tree using the leader IP and re-synchronize before attempting to create a new tree, this reduces network overhead.

Reference [19] have performed a wide range of simulations to test the performance of the MAODV protocol however a key limitation of their work is that they only used random waypoint mobility model in testing, as discussed previously this mobility model alone has several limitations. The simulations also failed to collect a number of important performance metrics such as network throughput and didn't perform any performance comparisons with other multicast protocols available such as Lightweight Adaptive Multicast (LAM) which were

discussed in the literature.

4. ISSUES OF AODV – SECURITY

One of the major concerns about deploying MANETs is security; wireless networks have increased vulnerability to a wide variety of security threats such as eavesdropping and packet tampering compared to traditional wired networks [7]. The original AODV protocol included no security mechanisms meaning that it is vulnerable to attacks which target the network routing protocol functions such as sequence number or hop count manipulation [21]. In order to address this issue researchers developed a number of security and authentication schemes for MANETs as well as extensions of AODV designed to increase security, such as Security-aware Ad-hoc On-demand Distance Vector (SAODV) and Adaptive Secure Ad-hoc On-demand Distance Vector (A-SAODV). These protocols feature digital signing of routing traffic and data to ensure integrity and authenticity.

4.1 Security-Aware Ad-Hoc on-Demand Distance Vector Routing Protocol (SAODV)

We reviewed literature produced by [22] which performed a comparison of three routing protocols; AODV, SAODV and A-SAODV. Security issues which these protocols address include Message tampering attacks, Message dropping attack and Message replay, also known as the wormhole attack. In

Attacks, AODV security protocols need the ability to authenticate and confirm the identity of a source. Protocols also need to authenticate the neighbor transmitting the packet; message integrity must also be checked to ensure that messages in transit have not been modified through accidental or malicious activity. Protocols need the ability to ensure that nodes wishing to access network resources have the appropriate access rights [22]. The literature includes performance simulations for the AODV, SAODV and A-SAODV protocols in a free-attack scenario where simulated threats attack the network. However the AODV protocol features no security mechanisms meaning this is not a fair comparison; the results for AODV should only be used as a benchmark for comparison. Simulations collected a number of important metrics but were only performed using a random waypoint mobility model with very high node speeds of 40m/s limiting the applicability of the results in a real world scenario as not many networks feature such high node speeds.

5 CONCLUSION

In this paper we have identified and reviewed a range of literature on the topic of MANET routing protocols, our initial work discussed a pair of survey papers from which we identified early reactive and proactive MANET routing protocols. Our review focuses upon protocols developed by Perkins, namely the Destination Sequenced Distance Vector (DSDV) and Ad-hoc On-demand Distance Vector (AODV) which researchers claim is the most popular MANET routing protocol. Due to the popularity of the AODV protocol a number of variations and improvements on the core protocol have been proposed by researchers to address specific issues with the protocol. We investigate the evolution of the AODV protocol by reviewing works based upon the Multicast Ad-hoc On-demand Distance Vector (MAODV), developed by [18], this protocol adds multicasting support to the core AODV protocol. A number of researchers highlighted the lack of security mechanisms within the original AODV protocol as a major concern for deployment of a MANET. We reviewed literature relating to the security of the

AODV protocol and proposed modifications with the aim of addressing the security issues raised, one example is the Security-aware Ad-hoc On-demand Distance (SAODV).

A common theme across many of the papers we have reviewed is the exclusive usage of random waypoint mobility model for simulations despite several researchers identifying limitations with this approach to testing. The collections of metrics from simulations is another area which was highlighted in several of the reviewed papers, researchers focus upon very specific metric collection but exclude collection of core metrics such as network throughput or delay which are essential for understanding the performance of a protocol. This is also true in the case of simulations which perform testing of protocols in isolation; this reduces the applicable value of the results because they cannot be directly compared to available alternatives.

REFERENCES

1. C. E. Perkins and E. M. Royer, "Multicast operation of the ad-hoc on-demand distance vector routing protocol," in Proc. of 5th annual ACM/IEEE international conference on Mobile computing and networking, Seattle, Washington, USA, August 15-20, pp. 207-218.
2. M. Zhang and P. H. J. Chong, "Performance Comparison of Flat and Cluster-Based Hierarchical Ad Hoc Routing with Entity and Group Mobility," in Proc. of IEEE Communications Society conference on Wireless Communications & Networking, Budapest, Hungary, 2009,pp. 2450-2455.
3. W. Wang and C. Amza, "Motion-based Routing for Opportunistic Ad-hoc Networks, "in Proc. of 14th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, October 31–November 4, 2011, pp. 169-178.
4. X. Hu, J. K. Wang, C. R. Wang, and C. Wang, "Is mobility always harmful to routing protocol performance of MANETs?" in Proc. of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 108-112, 2010.
5. B. Malarkodi, P. Gopal, and B. Venkataramani, "Performance evaluation of AD-hoc networks with different multicast routing protocols and mobility models," in Proc. of 2009 International Conference on Advances in Recent Technologies in Communication and Computing IEEE, India, 27-28 Oct., 2009, pp. 81-84.
6. C. Liu andS.Chang,"The study of effectiveness for ad-hoc wireless network," in Proc. of ICIS 2009 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 24-26 Nov., 2009, pp. 412-417.
7. B. Divecha, A. Abraham, C. Grosan, and S. Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models," in Proc. of First Asia International Conference on Modelling& Simulation, Phuket,Thailand, 27-30 March, 2007, pp. 224-229.
8. C.PerkinsandP.Bhagwat,"HighlyDynamicDestination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,"inProc. ofSigcomm conference on Communications architectures, protocols and applications, London, England, UK, 1994, pp. 234-244.
9. D. B. Johnson and D. A.Maltz,"Dynamic Source Routing in Ad Hoc Wireless Networks,"Mobile Computing, T. Imielinski and H. Korth, Ed. Kluwer Academic Publishers, 1996, vol. 5, pp. 153-181.

10. F. Maanand N. Mazhar, "MANET Routing Protocols vs Mobility Models: A Performance Evaluation," in Proc. of Third International Conference on Ubiquitous and Future Networks IEEE, Dalian, China, June 15-17, 2011, pp. 179-184.
11. C. E. Perkins and E. M.Royer," Ad-hoc On-Demand Distance Vector Routing," in Proc. of the 2nd IEEE workshop on mobile computing systems and applications, 1997, pp. 1-11.
12. W. A. Mobaideen, H. M. Mimi, F. A. Masoud, and E. Qaddoura, "Performance evaluation of multicast ad hoc on-demand distance vector protocol," Computer Communications, vol. 30, no. 9, pp. 1931–1941, 2007.
13. M. Mohammadizadeh, A. Moyaghar, and M. Safi, "SEAODV: Secure Efficient AODV Routing Protocol for MANETs Networks," in Proc. of2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, November 24-26,2009, pp. 940-944