RESEARCH PAPER | Computer Science | Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

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

KEYWORDS: Mens-rea,insanity,lunatic,unsoundness,offence,delusion,defence & Cognitive.

Mr. Jaydeep K. Morasana

Assistant Professor, Department of MCA, Atmiya Institute of Technology & Science - Rajkot, Yogidham gurukul, Kalawad Road, Rajkot – 360005 (Gujarat-India)

ABSTRACT *The characteristics of organization and wireless medium create Mobile unexpected NETwork (MANET) simple to line up and therefore enticing to users. The open and dynamic operational setting of painter makes it prone to numerous network attacks. a standard kind of attacks targets at the underlying routing protocols. Malicious nodes have opportunities to switch or discard routing data or advertise pretend routes to draw in user information to travel through themselves.*

Some new routing protocols are planned to deal with the problem of securing routing data. However, a secure routing protocol cannot single-handed guarantee the secure operation of the network in each state of affairs. The objectives of the thesis ar two-fold: (a) To simulate numerous situations of attacks at MANET; (b) to check the performance and effectiveness of some secure routing protocols in these simulated malicious situations, as well as Ariadne and also the Secure adhoc On-demand Distance Vector routing protocol (SAODV) .

1. Introduction

Many academic papers evaluate protocols and their abilities, assuming mobility within a restricted space, usually with all nodes .Different protocols are then calculated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. Network sizes and occurrences increased creating a requirement for inter-network communication. This led to the development of the Internet and its suite of protocols. The use of the Internet and its applications became ubiquitous. Research on MANETs has nearly 20 years focused on routing and this focus still remains. Numerous routing protocols for MANETs have been proposed and some surveys on these protocols have been published (2010) and an IETF Routing Area Working Group MANET (Mobile, 2011) has been active for a decade with six currently active Internet drafts. The following issues are main in this area:

1.1 Security

Mobile ad-hoc network operate in the absence of fixed infrastructure, which makes them easy to deploy. The absence of any fixed infrastructure in mobile ad-hoc networks makes it difficult to utilize and number of various challenges. Typical challenges like routing , bandwidth constraints, security and power. There are different proposed routing solutions for mobile ad-hoc networks which are table-driven, on-demand etc. Most of these solutions mainly focus on routing and do not concentrate security.

1.2 Protocol

Routing protocols can also be classified as link state protocols or distance-vector protocols. Routers using a link state routing protocol maintain a full or partial copy of the network topology and costs for all known links. Routers using a distance-vector protocol keep only information about next hops to adjacent neighbors and costs for paths to all known destinations. Generally speaking, "link state routing protocols are more reliable, easier to debug and less bandwidth-intensive than distance-vector" protocols. Link state protocols are also more complex and more compute- and memory-intensive. There are some previous protocols, such as the Source Tree Adaptive Routing (STAR) protocol and the Partial Tree-Sharing Protocol (PTSP), which are not the focus of active investigation now and their ideas are similar to more recently proposed protocols, such as the Topology Broadcast Based on Reverse-Path Forwarding (TBRPF) protocol.

1.3 Benefits

There are several advantages of MANET as it is wireless connection for information transfer from one place to another place with a very high speed and in huge amount of capacity which was unpredictable few years back. Transfers of real pictures have become activities of live telecast any incident to remote places.

1.4 Categories

There are different types of MANETs including:

InVANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.

Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipment's.

2. Review of various routing protocols for Mobile Ad-Hoc NETworks (MANET) :

I 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.

2.1 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

Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

[8] performed an extensive research survey into the available routing protocols and attempted to categorise 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.

2.2 Proactive Routing
Proactive protocols rely upon maintaining routing tables of known destinations, this cuts 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 neighbours, 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].

2.3 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].

2.3. Hybrid Routing
Hybrid protocols combine features from both reactive and proactive routing protocols, typically attempting to xploit 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. EARLY MANET ROUTING PROTOCOLS
The next part 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.

A. 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, this can add significant overhead to the network in dynamic scenarios [13].

B. 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].

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.

4.1. Ad-Hoc on-Demand Distance Vector (AODV) :
AODV utilizes sequence numbers and routing ideals 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

Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

simulation topology also uses a uniform random waypoint mobility model of 16 nodes which as discussed previously in Section 4. C is not an ideal testing environment.

4.2. Expanding upon AODV – Multicasting :
The AODV protocol is considered by some researchers [17] to be the most popular MANET routing protocol, this has lead to many alternatives and enhancements being proposed by researchers to address some of the many issues of wireless MANETs.

One of these issues was the lack of multicast support in early MANET routing protocols, including DSR, DSDV and

AODV, this functionality is useful for communicating with multiple nodes and increased available routing knowledge whilst reducing control traffic overheads [18]. In order to address this issue [18] proposed the Multicast Ad-hoc On-demand Distance Vector (MAODV) routing protocol, this protocol builds directly upon their previous work on AODV by adding support for multicast operation to the protocol.

The next piece of literature in our review is an evaluation of the MAODV protocol produced by [19] who discuss the technical aspects of the protocol and provides a number of simulations to evaluate the performance of the protocol in scenarios such as long and short lived communications.

4.2.1) Multicast ad-hoc on-demand distance vector (MAODV) :
The MAODV protocol shares the same underlying architecture as the AODV protocol with some modifications and the addition of Multicast Activations and Group Hello 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 synchronise 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-synchronise 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.

4.3 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 accept 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.

A. 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 an effort to guard against these attacks, AODV security protocols need the ability to authenticate and confirm the identity of a source. Protocols also need to authenticate the neighbour 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.

CONCLUSION :
In this paper i have identified and reviewed a range of literature on the topic of MANET routing protocols, my starting work discussed a pair of survey papers from which i identified early reactive and proactive MANET routing protocols. My 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.

I 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. I 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 I have reviewed is the exclusive usage of random way point 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 reduces the applicable value of the results because they cannot be directly compared to available alternatives.

Volume : 3 | Issue : 6 | June 2013 | ISSN - 2249-555X

REFERENCE

[1] E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 56, no. 2, pp. 940–965, October 2011. | [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] R. O. Schmidt and M. A. S. Trentin, "MANETs Routing Protocols Evaluation in a Scenario with High Mobility: MANET Routing Protocols Performance and Behaviour," Network Operations and Management Symposium, 2008. NOMS 2008. IEEE, Salvador, Bahia, pp.883-886, 2008. | [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] Y. Khamayseh, O. M. Darwish, and S. A. Wedian, "MA-AODV: Mobility Aware Routing Protocols for Mobile Ad hoc Networks," in Proc. of Fourth International Conference on Systems and Networks Communications IEEE, pp. 25-29, 2009. | [6] 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. | [7] R. Akbani, T. Korkmaz, and G .V. S. Raju, "HEAP: A packet authentication scheme for mobile ad hoc networks," Ad Hoc Networks, vol. 6, no. 7, pp. 1134–1150, 2008. | [8] A. Boukerche et al., "Routing protocols in ad hoc networks: A survey," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 55, no. 13. pp. 3032–3080, May 2011. | [9] B. Malarkodi, P. Gopal, and B. Venkataramani, "Performanceevaluation 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. | [10] H. Amri, M. Abolhasan, and T. Wysocki, "Scalability of MANET routing protocols for heterogeneous and homogenous networks," Computers and Electrical Engineering, vol. 36, no. 4, pp. 752–765, 2010. | [11] C. Liu and S. 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. | [12] 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. | [13] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in Proc. of Sigcomm conference on Communications architectures, protocols and applications, London, England, UK, 1994, pp. 234-244. | [14] 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.