A Study and Comparative Analysis of Wireless Routing Protocols

K.Murugan[1] Dr.P.Suresh[2] (Supervisor)

1. Research Scholar, Bharathiar University & Assistant Professor in Computer Science,, Govt. College for Women, Kolar, Karnataka, India, e-mail : mkcsresearch@gmail.com
2. HOD, Department of Computer Science, Salem SowdeswariCollege, Salem, Tamil Nadu, India, e-mail : sur_bh0071@rediffmail.com

Abstract

Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position. Wireless networks can be classified in two types: Infrastructures Network and Infrastructuresless Network. Infrastructures network consists of a network with fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach the base stations are fixed. It is expensive.Infrastructureless networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Ad hoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain. These routing protocols can be divided into two categories: table-driven and on-demand routing based on when and how the routes are discovered. In Table-driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables. On-demand routing protocols take a lazy approach to routing. In contrast to table-driven routing protocols all up-to-date routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed.

Keywords: Routing protocol, Table-driven, On-demand, Performance, Implementation

1. Review of Literature

1.1 Destination-Sequenced Distance-Vector (DSDV)

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the idea of the classical Bellman-Ford Routing Algorithm with certain improvements. Destination Sequenced Distance Vector. (DSDV) is a Proactive routing protocol that solves the major problem associated with the Distance Vector routing of wired networks i.e., Count-to-infinity, by using Destination sequence numbers. Destination sequence number is the sequence number as originally stamped by the destination. The DSDV protocol requires each mobile station to advertise, to each of its current neighbours, its own routing table (for instance, by broadcasting its entries). The entries in this list may change fairly dynamically over time, so the advertisement must be made often enough to ensure that every mobile computer can almost always locate every other mobile computer. In addition, each mobile computer agrees to relay data packets to other computers upon request. At all instants, the DSDV protocol guarantees loop-free paths to each destination.

1.2 Temporally Ordered Routing Algorithm (TORA)

The Temporally-Ordered Routing Algorithm (TORA) is an adaptive routing protocol for multihop networks that possesses the following attributes:

- Distributed execution
- Multipath routing
- The protocol can simultaneously support both source-initiated, on-demand routing for some destinations and destination-initiated, proactive routing for other destinations.
- Minimization of communication overhead via localization of algorithmic reaction to topological changes.

TORA is a distributed routing protocol based on a "link reversal" algorithm. Route optimality (shortest-path routing) is considered of secondary importance, and longer routes are often used to avoid the overhead of discovering newer routes.TORA is distributed, in that routers need only maintain information about adjacent routers (i.e., one-hop knowledge). Like a distance-vector routing approach, TORA maintains state on a per-destination basis. However, TORA does not continuously execute a shortest-path computation and thus the metric used to establish the routing structure does not represent a distance. The destination-oriented nature of the routing structure in TORA supports a mix of reactive and proactive routing on a per-destination basis. During reactive operation, sources initiate the establishment of routes to a given destination on-demand. This mode of operation may be advantageous in dynamic networks with relatively sparse traffic patterns, since it may not be necessary (or desirable) to maintain routes between every source/destination pair at all times. At the same time, selected destinations can initiate proactive operation, resembling traditional table-driven routing approaches. This allows routes to be proactively maintained to destinations for which routing is consistently or frequently required (e.g., servers or gateways to hardwired infrastructure). TORA is designed to minimize the communication overhead associated with adapting to network topological changes.

1.3 **Dynamic Source Routing (DSR)**

Dynamic Source Routing (DSR) is a reactive protocol i.e. it doesn't use periodic advertisements. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass; the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.

There are two significant stages in working of DSR: Route Discovery and Route Maintenance. A host initiating a route discovery broadcasts a *route request* packet that may be received by those hosts within wireless transmission range of it. The route request packet identifies the host, referred to as the *target* of the route discovery, for which the route is requested. If the route discovery is successful the initiating host receives a *route reply* packet listing a sequence of network hops through which it may reach the target. In addition to the address of the original initiator of the request and the target of the request, each route request packet contains a *route record*, in which is accumulated a record of the sequence of hops taken by the route request packet as it is propagated through the network during this route discovery.While a host is using any source route, it monitors the continued correct operation of that route. This monitoring of the correct operation of a route in use is called *route maintenance*. When route maintenance detects a problem with a route in use, route discovery may be used again to discover a new, correct route to the destination.

1.4 Adhoc On-Demand Distance Vector Routing (AODV)

Adhoc On-demand Distance Vector (AODV) is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. It uses destination sequence numbers to ensure loop freedom at all times and by avoiding the Bellman-Ford ”count-to-infinity” problem offers quick convergence when the ad hoc network topology changes, Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies.

As long as the endpoints of a communication connection have valid routes to each other, AODV does not play any role. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is a valid route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. The route is made available by unicasting a RREP back to the origination of the RREQ. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator, or likewise from any intermediate node that is able to satisfy the request.

2. Performance Metircs and Implementation

2.1 Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the CBR sources.Calculate the number of “sent packets” that have the trace form:

```
/^s *- Nl AGT.*-Is (\d{1,3})\.\d{1,3} -Id
(\d{1,3})\.\d{1,3}.*-It cbr.*-Ii (\d{1,6})/
```

AGT => Agent Level Trace.Calculate the number of “received packets” of the trace form:

```
/^r -t (\d{1,3}\.\d{9}).*-Nl AGT.*-Is
(\d{1,3})\.\d{1,3} -Id (\d{1,3})\.\d{1,3}.*-It cbr.*-Ii
(\d{1,6})/
```

packet delivery fraction (pdf %) = (received packets/ sent packets) *100

2.2 Average End-to-End Delay of Data Packets

This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.For each packet with id (Ii) of trace level (AGT) and type (cbr), calculate the send(s) time (t) and the receive (r) time (t) and average it.

2.3 Normalized Routing Load

The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.The first two metrics are the most important for best-effort traffic. The routing load metric evaluates the efficiency of the routing protocol. Note, however, that these metrics are not completely independent. For example, lower packet delivery fraction means that the delay metric is evaluated with fewer samples. In the conventional wisdom, the longer the path lengths, the higher the probability of a packet drops. Thus, with a lower delivery fraction, samples are usually biased in favor of smaller path lengths and thus have less delay. Calculate the routing packet sent:

```
/^[s|f].*-Nl RTR.*-It
(?:AODV|DSR|message) -Il (\d{1,4})/
```

f=> forward

RTR=> Routing Trace Level

Normalized routing load = (routing packets sent) / receives.

The new trace format looks like:

```
s -t 0.267662078 -Hs 0 -Hd -1 -Ni 0 -Nx 5.00 -Ny 2.00 -Nz 0.00 –
Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 –Ii 20 -
Is 0.255 -Id -1.255 –It
```

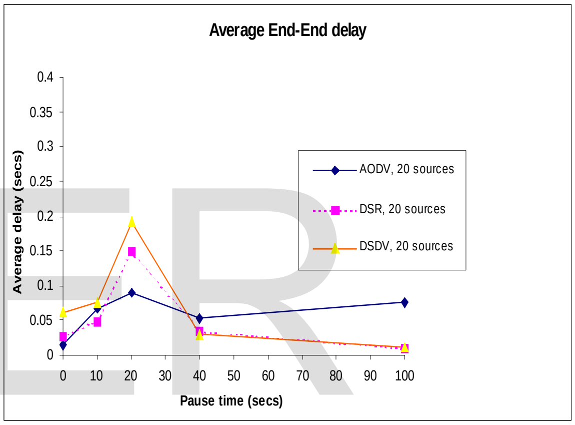
Here, we see that a packet was sent (s) at time (t) 0.267662078 sec, from source node (Hs) 0 to destination node (Hd) 1. The source node id (Ni) is 0, its x-co-ordinate (Nx) is 5.00, it’s y-co-ordinate (Ny) is 2.00, it’s z-co-ordinate (Nz) is 0.00, it’s energy level (Ne) is 1.000000, the trace level (Nl) is RTR and the node event (Nw) is blank. The MAC level information is given by duration (Ma) 0, destination Ethernet address (Md) 0,the source Ethernet address (Ms) is 0 and Ethernet type (Mt) is 0. The IP packet level information like packet id (Ii), source address.source port number is given by (Is) while the destination address. destination port number is (Id).

3. Result and Discussion

First, an attempt was made to compare all the 4 protocols under the same simulation environment. However, simulations couldn't be successfully carried out for the TORA routing protocol, as matlab repeatedly gave a bus error while running the TORA simulations. For all the simulations, the same movement models were used, the number of traffic sources was fixed at 20, the maximum speed of the nodes was set to 20m/s and the pause time was varied as 0s, 10s, 20s, 40s and 100s.

The following figure highlights the relative performance of the three routing protocols. All of the protocols deliver a greater percentage of the originated data packets when there is little node mobility (i.e., at large pause time), converging to 00% delivery when there is no node motion.The simulation results bring out some important characteristic differences between the routing protocols.The presence of high mobility implies frequent link failures and each routing protocol reacts differently during link failures. The different basic working mechanism of these protocols leads to the differences in the performance.

DSDV fails to converge below lower pause times. At higher rates of mobility (lower pause times), DSDV does poorly, dropping to a 70% packet delivery ratio. Nearly all of the dropped packets are lost because a stale routing table entry directed them to be forwarded over a broken link. As described in the earlier section, DSDV maintains only one route per destination and consequently, each packet that the MAC layer is unable to deliver is dropped since there are no alternate routes. For DSR and AODV, packet delivery ratio is independent of offered traffic load, with both protocols delivering between 85% and 100% of the packets in all cases.



Since DSDV uses the table-driven approach of maintaining routing information, it is not as adaptive to the route changes that occur during high mobility. In contrast, the lazy approach used by the on-demand protocols, AODV and DSR to build the routing information as and when they are created make them more adaptive and result in better performance (high packet delivery fraction and lower average end-to-end packet delays).

4. Conclusion

The performance of DSDV, AODV and DSR routing protocols for ad hoc networks using mat lab. DSDV uses the proactive table-driven routing strategy while both AODV and DSR use the reactive On-demand routing strategy. Both AODV and DSR perform better under high mobility simulations than DSDV. High mobility results in frequent link failures and the overhead involved in updating all the nodes with the new routing information as in DSDV is much more than that involved AODV and DSR, where the routes are created as and when required.DSR and AODV both use on-demand route discovery, but with different routing mechanics.

In particular, DSR uses source routing and route caches, and does not depend on any periodic or timer-based activities. DSR exploits caching aggressively and maintains multiple routes per destination. AODV, on the other hand, uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes. The general observation from the simulation is that for application-oriented metrics such as packet delivery fraction and delay AODV, outperforms DSR in more "stressful" situations (i.e., smaller number of nodes and lower load and/or mobility), with widening performance gaps with increasing stress(e.g., more load, higher mobility). DSR, however, consistently generates less routing load than AODV.

5. References

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Volume 60, Issue 3, March 2013, Pages 1089 – 1098

[2] ConstantinosKolias, Vasilis Kolias, GeorgiosKambouraki, "TermID: a distributed swarm intelligence-based approach for wireless intrusion detection", International Journal of Information Security, Springer, 2016, Pages 1–16

[3] Bandana Mahapatra, Srikanta Patnaik, "Self Adaptive Intrusion Detection Technique Using Data Mining concept in an Ad-Hoc Network", Procedia Computer Science, Elsevier, Volume 92, 2016, Pages 292 – 297

[4] AikateriniMitrokotsa a, Christos Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Ad Hoc Networks, Elsevier, Volume 11, 2013, Pages 226–237

[5] M. Usha ,P. Kavitha, "Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier", wireless networks, Springer, Pages 1-16

[6] SannasiGanapathy, KanagasabaiKulothungan, SannasyMuthurajkumar, Muthusamy Vijayalakshmi, Palanichamy Yogesh and Arputharaj Kannan, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey" EURASIP Journal on Wireless Communications and Networking, 2013, Pages 1-16

[7] Vishnu Balan E, Priyan M K, Gokulnath C, Usha Devi G, "Fuzzy Based Intrusion Detection Systems in MANET", Procedia Computer Science, Elsevier, Volume 50, 2015, Pages 109 – 114

[8] Binod Kumar Pattanayak and MamataRath, "Mobile Agent based Intrusion Detection System Architecture for Mobile Ad hoc Networks", Journal of Computer Science, Volume 10 Issue 6, 2014, Pages 970-975

[9] Vydeki, D., and Bhuvaneswaran, R. S., "Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks", Journal of Computer Science, Volume 9, Issue 4, 2013, Pages 521-525.

[10] BasantSubba, Santosh Biswas , SushantaKarmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation", Engineering Science and Technology, an International Journal, Elsevier, Volume 19, 2016, Pages 782–799

[11] Sungwook Kim, "Adaptive MANET Multipath Routing Algorithm based on the Simulated Annealing Approach",

Hindawi Publishing Corporation, The Scientific World Journal, Volume 2014, May 2014, Pages 1-9.

[12] KonagalaPavani and AuvulaDamodaram,. “Multi-class Intrusion Detection System for MANETs”, Journal of Advances in Computer Networks, Volume 3, Issue 2, June 2015, Pages 93-98

[13] S. Ganapathy, P. Yogesh, and A. Kannan, “Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM”, Computational Intelligence and Neuroscience, Hindawi Publishing Corporation, Volume 2012, May 2014, Pages 1-10

[14] Alka Chaudhary, V. N. Tiwari, and Anil Kumar, “A New Intrusion Detection System Based on Soft Computing Techniques Using Neuro-Fuzzy Classifier for Packet Dropping Attack in MANETs”, International Journal of Network Security, Volume 18, Issue 3, May 2016, Pages 514-522

[15] Chun-Wei Tsai, “Incremental particle swarm optimization for intrusion detection”, IET Networks, Volume 2, Issue 3, 2013, Pages 124 – 130.