TODV: Performance Analysis of a Time on Demand Distance Vector Protocol for MANETS

G.S. Mamatha
Assistant Professor, ISE Dept.
R.V. College of Engineering
Bangalore

Dr. S.C. Sharma
Vice Chancellor
Tumkur University
Tumkur, Karnataka

ABSTRACT
In MANET (Mobile Adhoc Network) the physical connectivity of the network keeps on changing dynamically. Because of the several MANET constraints such as limited bandwidth, mobility, battery power etc; it becomes very important to design a protocol that suits the requirements for MANETS. In this paper, we suggest a protocol mechanism which is loosely based on a reactive protocol AODV (Ad Hoc On demand Distance Vector Protocol). The proposed protocol uses the time concept based on first come first served basis for path choosing process, hence the name Time On Demand Distance Vector Protocol (TODV). The protocol design presented here suits the MANETS dynamic topology perfectly in finding the best path or route for data communication. The simulation study reveals that the proposed protocol outperforms than existing AODV, in terms of throughput and end-to-end delay.

General Terms
MANET, AODV, TODV, Time, Protocol

Keywords
Mobile ad hoc network, protocol, communication, time.

1. INTRODUCTION
The basic threats for packet forwarding and routing in MANETS are attacks. MANETS cannot be made free of attacks since it is infrastructure less, dynamic topology and no centralized control. The basic function that is carried by any of the network is routing and packet forwarding. For packet forwarding in the network the nodes will depend on each other because of their limited number in the transmission range. As a result, embedding solutions in routing protocols to handle attacks poses a challenge to the researchers [1]. Basically the routing threats due to attacks in MANETS are mainly because of malicious nodes [2] and selfish nodes [3]. Malicious nodes mainly launch attacks solely to disturb the normal functioning of the network by performing some harmful operations at the cost of their battery life whereas selfish nodes do not cooperate in the normal functioning of the network to save their battery life for their own communication. Malicious nodes can cripple the network by inserting erroneous replaying old routing information, changing routing updates, or advertising incorrect routing information so that the network is not able to provide service properly. Attacks like reducing the amount of routing information available to other nodes, failing to advertise certain routes or discarding routing packets or parts of routing packets are due to selfish behavior of a node. Two main approaches are used to make routing protocols handle attacks in ad hoc networks. The first approach aims at detecting the malicious nodes while computing the route in the network and re-routing the packets around it, mostly along the shortest path among them. Most of these protocols [4, 5, 6, 7, 8, 9, 10, 11 and1] are based on existing ad hoc routing protocols like AODV [12], DSDV [13] and DSR [14], redesigned to handle attacks. The second approach [15, 16, 17] separates the detection of malicious nodes from routing [1].

Albeit designing a routing protocol is a major challenge in MANETS, since it involves certain issues which have to be covered. The main issues are mobility, bandwidth constraint, hidden and exposed terminal problems, shared broadcast channel, resource constraints and others. When designing a routing protocol some of the characteristics should be considered as follows [18]:

- The routing protocol should be distributed in nature, so that it will be more fault tolerant than centralized routing.
- The network is dynamic in nature due to frequent topological changes and mobility of nodes.
- The number of nodes in the network should be less and involves least complexity in computing routes and maintenance. Access to routes should be easy and connection setup should be fast.
- The routing protocol should be loop free and free from stale routes.
- The transmissions should be reliable, which reduces message loss and collisions.
- The usage of resources like bandwidth, computing power, memory and battery should be used optimally.
- The topological information that changes frequently should be maintained by all the nodes in the network.
- The protocol should be time sensitive for specific applications.

The main criterion considered in this paper is that the protocol is mainly based on the routing information update mechanism, which is called reactive or on-demand routing protocols. In these protocols no topological information will be maintained. The path set up will take place only when the nodes want to communicate. Hence there will be no frequent updating of routing information in the network. One such on demand routing protocol is AODV, which can be the basis for designing similar protocols which can tackle the ad hoc issues to the greater extent.

2. RELATED WORK
The need for a secure routing protocol or a mechanism to overcome the misbehavior problem of wireless networks including MANETs has been studied by many researchers. Various protocols and schemes have been proposed to prevent malicious activities in MANETs.

Marti et al. [19] Proposed a watchdog and pathrater schemes to improve the throughput of MANET in the presence of misbehaving node. To keep tracking of misbehaving nodes watchdog is used and to abandon routing process through the misbehaving nodes pathrater is applied. Yang et al. [20] proposed an extended version of AODV with a self –organized security approach. Here a node only with valid token, can participate in the route discovery and data packet delivery.

Collaborative Voting System (CVS) is another mechanism proposed to overcome limitations of watchdog mechanism. This approach has some constraints like computational overhead which will consume more energy and communication overhead which will increase network traffic. Later Zhong proposed a credit-based scheme, termed Sprite [21]. In Sprite, nodes keep receipts of the received/forwarded messages. In the network architecture of Sprite, the CCS (Credit Clearance Service) is assumed to be reachable through the use of the Internet, limiting the utility of Sprite.

The CONFIDANT protocol proposed by Buchegger and Le Boudec in [9] is an example of reputation-based schemes. The protocol is based on selective altruism and utilitarianism, thus making misbehavior unattractive. CONFIDANT consists of four important components - the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighborhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. The scheme has got the same problems as that of watchdog scheme.

The 2ACK scheme proposed by K. Balakrishnan et al. [22] does not rely on end-to-end acknowledgment. Such an acknowledgment scheme may not exist in some traffic flows (such as UDP). Instead, the 2ACK scheme tries to detect misbehaving links as the links are being used. Since it is a proactive detection approach, it needs faster and quicker detection of misbehaving links. Kejun Liu et al. [23] proposed another 2ACK scheme to mitigate the adverse effects of misbehaving nodes. The basic idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully, which is only for a fraction of data packets to reduce overhead.

Dhaval gada et al. [24] proposed a scheme related to the number of RREQ's (route requests). In original AODV, a malicious node can override the restriction put by RREQ_RATELIMIT [25] parameter (limit of initiating /forwarding RREQs) by increasing or disabling it. A node in the network can able to do so because of its self-control over its parameters. The default value for the RREQ_RATELIMIT parameter is 10 as proposed by RFC 3561. A compromised or a malicious node may choose to set the value of parameter RREQ_RATELIMIT to a very high number. This allows it to flood the network with fake RREQs [25] and lead to a kind of DoS attack. In this type of DoS attack a non-malicious node cannot fairly serve other nodes due to the network-load imposed by the fake RREQs. This leads to the problems such as bandwidth wastage, creating more overhead by wasting the nodes processing time, exhaustion of the network resources like memory (routing table entries), exhaustion of the node's battery power. These underperformances further leads to degraded throughput. Most of the network resources are wasted in trying to generate routes to destinations that do not exist or routes that are not going to be used for any communication. This implies that the existing version of AODV is vulnerable to such type of malicious behavior from an internal node (which can be a compromised node, malicious node or a selfish node).

To overcome a sort of problems not all we are proposing a mechanism which is mainly based on topology of MANETS and reduces the time consumed in path detection process the RREQ limit in the proposed scheme is not set unlike in AODV, but it is left to the usage choice and depends on the network density also. For the proposed work the limit has been set to 3 i.e. a node can send RREQ to any 3 of its neighbors considering 30 and 50 node capacity network. The proposed scheme is incurring very less overhead, as it makes minimal modifications to the existing data structures and functions related to blacklisting a node in the existing version of pure AODV (RFC 3561). Secondly the proposed scheme is more efficient in terms of its resultant routes established, resource reservations and its computational complexity. Thirdly, the mechanism successfully avoids the occurrence of more than one malicious node to participate in active routing process.

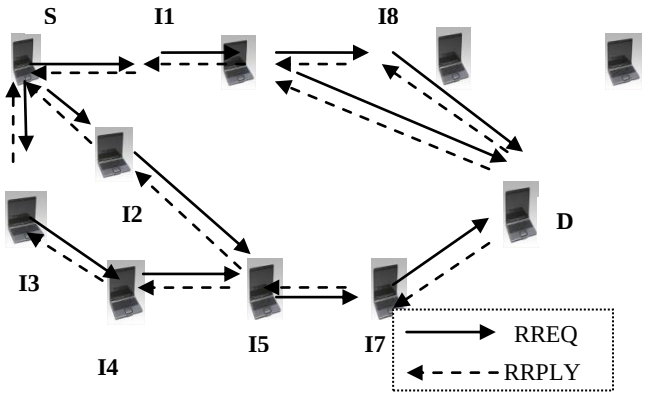
We are yet to evaluate few attacks against AODV routing protocol and the proposed protocol in future and also check for the defensive approach applied on the mechanism proposed.

3. PROTOCOL DESCRIPTION

This paper concentrates on one of the reactive protocol that is AODV [26] (Ad hoc on demand distance vector protocol) which uses an on demand approach to find routes. The route will be active only when the source node is ready to send some data packets. The original AODV uses destination sequence numbers to identify the most recent path. The source node and intermediate nodes contain the next hop information for packet transmission. The policy of an on demand protocol is that the source node floods the Route Request (RREQ) whenever it sends data through the network, since the source couldn't find any routes to forward the data. In the process of finding route there may be possibility of finding several routes to destination. According to original AODV the path is found by using destination sequence number. Whichever the route is having the highest destination sequence number compared to that of last stored, the path will be get selected for data transmission.

A slighter modification to the existing AODV protocol has been considered in this paper. The RREQ carries Source Identifier (SID), Destination Identifier (DID) and a Route Node Collection packet (RNC). The SID denotes the source address, DID denotes the destination address and the RNC packet contains the intermediate node IDs address through number of hops as shown in figure 1. That is the RNC packet gives the route definition with total number of hops defined to every node it has visited. As mentioned earlier the limit for RREQ is 3 set for any of the source node, which starts flooding RREQs through the network. Once the RREQ reaches every node, it checks the DID with itself and if not matched forwards further to the next neighboring nodes. In this modified protocol version the RNC packet has different route node collection information. Every node maintains route information about the neighboring nodes. Every RREQ to a destination node generates a Route Reply (RRPLY) packet. The RRPLY packet contains a SID, DID and a RNC packet. Here the notations change, as the SID denotes the destination node address, DID refer to the source node address and RNC again gives the

route information it has collected through the RREQ process. In RRPLY DID takes data from RNC to which node it has to pass the RRPLY until it reaches source node. The RRPLY will come from different routes to source node. The first come first served basis is applied here instead of considering the destination sequence number concept. The RRPLY which arrives first, means which takes minimum time to reach source node will be the shortest path in that instance of time; this is because the MANET topology is dynamic in nature. To count the time of every RRPLY that arrives back to source node a clock will be set at the chosen source node. As the next step the path chosen will be considered for data communication between source and destination nodes. Parallely the other alternative routes possible will also be maintained in database, in case if first route is proved to be malicious.



S-Source, D-Destination, I1 to I8-Intermediate nodes
Consider RREQ1 from S to I1:
RREQ1: (SID, DID, **RNC= ({S → I1 → D}, 3Hops)**)
RREQ1: (SID, DID, **RNC= ({S → I1 → I6 → D}, 4Hops**))
RRPLY1: (DID, SID), {D → I6 → I1 → S})
RRPLY1: (DID, SID), {D → I8 → I6 → I1 → S}

Figure 1: A Scenario of MANET showing the contents of RNC Packet.

The structure of RREQ in the designed TODV protocol is as shown in table 1:

Table 1: RREQ Packet

DID=source node	SID=destination node	RNC

The structure of RRPLY in the TODV protocol is as shown in table 2:

Table 2: RRPLY Packet

SID	DID	RNC

3.1 Performance Evaluation

The metrics for evaluating the performance of the TODV protocol are as follows for detailed routing protocol analysis.

• Throughput – It is defined as the total useful data received per unit of time.

• End-to-End Delay (Path Optimality) – the difference between the numbers of hops a packet took to reach its destination and the length of the shortest path that physically existed through the network when the packet was originated.

The protocol is checked for the misbehaving links by launching attacks on a selected route. In such cases the acknowledgments from the destination are carrying some message indicating misbehavior or missing. Because of this the source node of a TCP session may slow down or even stop sending packets. Therefore, a more reasonable performance metrics is the total number of packets that are received at the destination. The comparison is made between end to end delay, normalized number of packets that are received, of AODV and the TODV protocol in the TCP traffic scenario.

3.2 Simulation Environment

To analyze the TODV protocol, a real time simulation is conducted by using a simulator designed and developed at the par to standard available simulators. The wireless transmission range of each node was 250 m. Traffic sources of constant bit rate (CBR) based on TCP have been used. The CBR and TCP mobility scenario of 30 and 50 nodes with maximum speed of 10m/sec and for simulation area of 100 x 70 flat area is conducted. For each data entry with 4 bytes and 8 bytes, 5 simulation runs were conducted to obtain the average value.

The snapshot in figure 2 indicates packet transmissions among nodes within the power range. For the AODV protocol block, main events of concern are the Route request, Route reply and data packets.

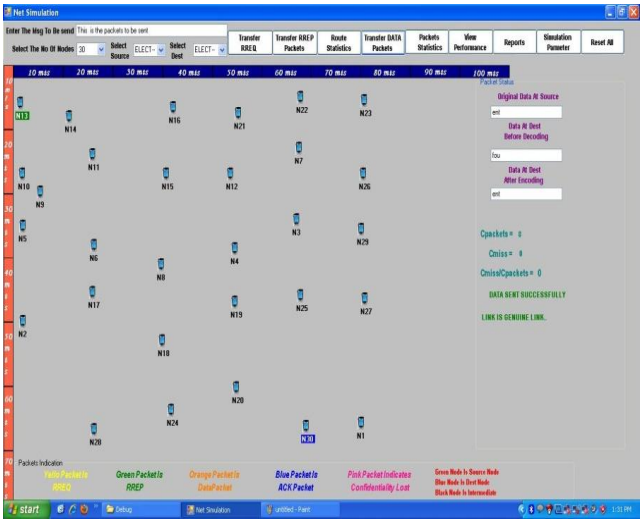


Figure 2: Simulation Environment

4. SIMULATION RESULTS

The simulation results of AODV and TODV are as follows:

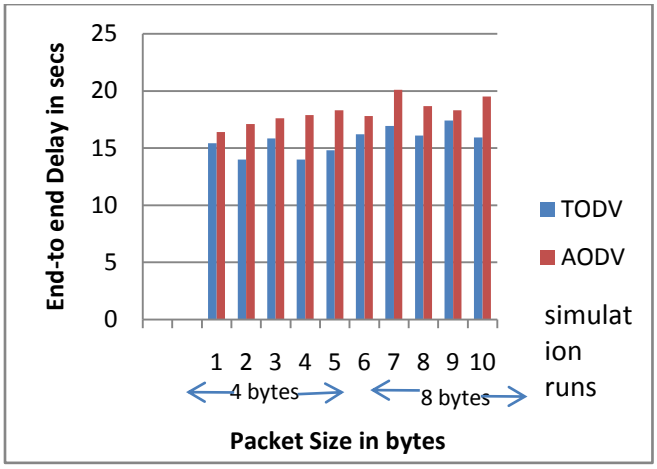


Figure 3: End-to-end Delay of TODV and AODV

Figure 3 shows the average end to end delay of the proposed TODV protocol with AODV. For less number of bytes the AODV shows consistent performance in delay and increased delay when number of bytes is raised to 8. We can observe that the delay will be more for AODV than the proposed protocol with 30 node density network. The end to end delay increases as the bytes are increased in case of AODV protocol. Compared with the AODV scheme, the proposed protocol shows much lesser end-to-end delay.

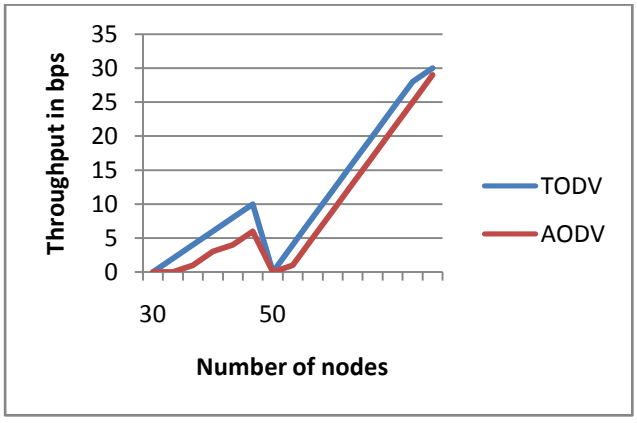


Figure 4: Throughput of TODV and AODV

In Figure 4, we present the relative throughput, normalized number of packets received, when the proposed TODV protocol and AODV are used. The relative throughput reduces for both TODV protocol and AODV when the number of nodes is increased from 30 to 50 and then again increases. Also, we can observe that the proposed protocol outperforms AODV in terms of relative throughput, especially in the networks with larger number of nodes.

When compared to original AODV, the proposed protocol TODV based on AODV works with respect to time constraint rather considering the destination sequence number concept. The advantage of this protocol is whichever RRPLY comes faster i.e. with minimum time, that route will be chosen as the best route. This reduces the complexity of assigning sequence numbers for nodes and calculation of highest sequence number of routes.

5. CONCLUSION

As AODV is one of the best reactive routing protocols for MANETS, this attempt is just a minor contribution towards designing new protocol suite. The time concept will reduce the complexity of calculation of sequence numbers. The performance of the TODV protocol ensures that it is outperforming than AODV. Further the research can be continued in finding out whether the protocol is against attacks to make it robust in nature. The number of network metrics can be increased to measure the performance of the protocol proposed as the next step towards the research work

6. ACKNOWLEDGMENTS

My sincere thanks to my honorable guide Dr. S. C. Sharma and others who have contributed towards the preparation of the paper.

7. REFERENCES

[1] Sandhya Khurana, Neelima Gupta, Nagender Aneja, "Minimum Exposed path to the Attack (MEPA) in Mobile Ad Hoc Network (MANET)" In proceedings of ICN '07, Sixth International conference on Networking, IEEE Computer Society, 2007.

[2] Matthias Hollick, Jens Schmitt, Christian Seipl, and Ralf Steinmetz "On the Effect of Node Misbehavior in Ad Hoc Networks", http://disco.informatik.uni-kl.de/publications/HSSS04-2.pdf.

[3] Pietro Michiardi and Refik Molva "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks" http://www.eurecom.fr/michiard/pubs/mimo02-EW2002.pdf.

[4] P. Papadimitratos, Z. Haas, "Secure Routing for Mobile Ad Hoc Networks", Proceedings of CNDS 2002.

[5] Y-C Hu, A. Perrig, D. B. Johnson, "Ariadne : A secure On-Demand Routing Protocol for Ad Hoc Networks", in proceedings of MOBICOM 2002.

[6] B. Dahill, B. N. Levine, E. Royer, C. Shields, "ARAN: A secure Routing Protocol for AdHoc Networks", UMass Tech Report 02-32, 2002.

[7] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks", Proceedings of the 4th IEEEWorkshop on Mobile Computing Systems & Applications (WMCSA 2002), IEEE, Calicoon, NY, 2002.

[8] L. Buttyan, J.-P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in selforganized ad hoc networks", Technical Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne, 2001.

[9] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)", Proceedings of The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, 9-11 June, 2002, Lausanne, Switzerland, ACM Press, 2002, pp. 226-236.

[10] Pietro Michiardi and Refik Molva, "CORE: A COllaborative REputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia., 2002.

[11] Seung Yi, Prasad Naldurg, Robin Kravets, "A Security-Aware Routing Protocol for Wireless Ad Hoc Networks", Proceedings of 6th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI), Orlando, FL, July 2002, pp. 286-292.

[12] Charles E. Perkins, Elizabeth M. Belding Royer and Samir R. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing", Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt, February 2003.

[13] Charles E. Perkins and Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, August 1994, pp. 234-244.

[14] D. B. Johnson, D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[15] Yongguang Zhang and Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks" Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (Mobi-Com'2000), August 6-11,2000, Boston, Massachussetts.

[16] Yi-an Huang,Wenke Lee,"A Cooperative Intrusion Detection System for Ad Hoc Networks", Proceedings of the First ACM Workshop Security of Ad Hoc and Sensor Networks Fairfax, Virginia.

[17] Yongguang Zhang, Wenke Lee, Yi-an Huang, "Intrusion Detection Techniques for Mobile Wireless Networks" Wireless Networks 9,545-556,2003,_c 2003 Kluwer Academic Publishers.

[18] C. Siva Ram Murthy, B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Low Price Edition, Pearson Education, 2007.

[19] S.Marti, T. J. Giuli, K. Lai, and M. Baker, " Mitigating routing misbehavior in mobile ad hoc networks.In Mobile Computing and Networking", pages 255–265,2000. Also available as http://citeseer.nj.nec.com/marti00mitigating.html

[20] H.Yang, X.Meng, and S.Lu, " Self-organized network layer security in mobile ad hoc networks", in Workshop on Wireless Security (Wise'02), Septemper 2002.

[21] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof,Credit-Based System for Mobile Ad-Hoc Networks," Proc.INFOCOM, Mar.- Apr. 2003

[22] K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK:Preventing Selfishness in Mobile AdHoc Networks," Proc. IEEEWireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[23] Kejun Liu, Jing Deng, , Pramod K. Varshney, and Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," In IEEE Transactions On Mobile Computing, pages 488 – 502,VOL. 6, NO. 5, MAY 2007.

[24] Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia, Nirali Mody, Sugata Sanyal and Ajith Abraham. "A Distributed Security Scheme for Ad Hoc Networks", ACM Publications, Vol-11, Issue 1, pp.5–5, 2004.

[25] Perkins C.E., Terminology for Ad-Hoc Networking, Draft-IETF-MANET-terms-00.txt, November 1997.

[26] C.E. Perkins, E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of IEEE Workshop on Mobile Computing systems and Applications 1999, pp. 90-100, February 1999.