An Improved DSDV Routing Protocol For Wireless Ad Hoc Networks

Gulfishan Firdose Ahmed\textsuperscript{a}, Raju Barskar\textsuperscript{b}, and Nepal Barskar\textsuperscript{c}

\textsuperscript{a} Research Scholar, CSE & IT Department
Maulana Azad National Institute of Technology, Bhopal (M.P.) Pin-462051, India.
\textsuperscript{b} Research Scholar, CSE & IT Department
Maulana Azad National Institute of Technology, Bhopal (M.P.) Pin-462051, India.
\textsuperscript{c} Student of BE, CSE Department, University Institute of Technology,
Rajiv Gandhi Prodhyogiki Vishvidyalaya, Bhopal (M.P.) Pin-462036, India.

Abstract

A Mobile Ad hoc NETwork (MANET) is a kind of wireless ad-hoc network and is a self configuring network of mobile routers connected by wireless links. The wireless links form the union of an arbitrary topology. There are various routing protocols available for MANETs. The most popular ones are DSR, AODV and DSDV. This paper examines routing protocol for mobile ad hoc networks--the Destination Sequenced Distance Vector (DSDV) and On-Demand protocol that evaluates both protocols based on the packet delivery fraction and average delay while varying number of sources and pause time. In this paper we consider the new approach an Improved-DSDV Protocol is proposed for Ad Hoc networks. Improved-DSDV overcomes the problem of stale routes, and thereby improves the performance of regular DSDV. The proposed protocol has been implemented in the NS-2 Simulator and performance comparison has been made with regular DSDV and improved DSDV protocols. We compare the performance of our work with DSDV. In our improved DSDV routing protocol, nodes can cooperate together to obtain an objective opinion about another node’s trustworthiness. The performance metrics considered are packet-delivery ratio.

1. Introduction

In the integrated MANET-Internet communication, a connection could be disrupted either by attacks on the Internet connectivity or by attacks on the ad hoc routing protocols. Because of this almost all possible attack on the traditional ad hoc networks also exist in the integrated wired and mobile ad hoc networks [1]. The other factors which need to be considered while choosing a protocol for MANETs are as follows [9-12]:

\begin{itemize}
\item [\textsuperscript{1}] Improved-DSDV
\item [\textsuperscript{2}] Security
\item [\textsuperscript{3}] DSDV
\end{itemize}
Multicasting: This is the ability to send packets to multiple nodes at once. This is similar to broadcasting except the fact that the broadcasting is done to all the nodes in the network. This is important as it takes less time to transfer data to multiple nodes.

Loop Free: A path taken by a packet never transits the same intermediate node twice before it arrives at the destination. To improve the overall, we want the routing protocol to guarantee that the routes supplied are loop-free. This avoids any waste of bandwidth or CPU consumption.

Multiple routes: If one route gets broken due to some disaster, then the data could be sent through some other route. Thus the protocol should allow creating multiple routes.

Distributed Operation: The protocol should of course be distributed. It should not be dependent on a centralized node.

Reactive: It means that the routes are discovered between a source and destination only when the need arises to send data. Some protocols are reactive while others are proactive which means that the route is discovered to various nodes without waiting for the need.

Unidirectional Link Support: The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance[13].

Power Conservation: The nodes in an ad-hoc network can be laptops and thin clients, such as PDAs that are very limited in battery power and therefore use some sort of standby mode to save power. It is therefore important that the routing protocol has support for these Sleep-modes [2-3].

2. Related work

A lot of research has been carried out in both the route discovery security part of routing protocols, and on packet forwarding. This Section at first looks at different ways of securing the network against misbehaving nodes and data forwarding anomalies. Then a sneak review followed shows the work that attempts to identify and prevent misbehavior in data packet forwarding.

Secure routing protocols have been proposed based on existing ad hoc routing protocols. These eliminate some of the optimizations introduced in the original routing protocols because they can be exploited to launch different types of attacks. Examples of such protocols are the secure efficient distance vector (SEAD) routing [5] which is based on the destination sequenced distance vector (DSDV) [5], the secure ad-hoc on-demand distance vector (SAODV) routing protocol [8] [9] based on AODV [10] [11], and the secure on-demand routing protocol for ad hoc networks (Ariadne) [12] based on the dynamic source routing (DSR) protocol [13] and the timed efficient stream loss-tolerant authentication (TESLA) protocol proposed in [14]. Also extending DSR to provide it with security mechanisms is CONFIDANT (Cooperation of Nodes: Fairness In Dynamic Ad-hoc NetWorks) [15]. These approaches only secure the path discovery and establishment functionality of routing protocols, thus the proposed approach complements them by securing the data forwarding functionality [1].

WATCHERS (Watching for Anomalies in Transit Conservation: a Heuristic for Ensuring Router Security) [4] is a protocol designed to detect disruptive routers in fixed networks through analysis of the number of packets entering and exiting a router. In this approach each router executes the WATCHERS protocol at regular intervals in order to identify neighboring routers that misroute traffic and avoid them. SCAN (self-organized network layer security in mobile ad hoc networks) [3] focuses on securing packet delivery. It uses AODV [10] [11], but argues that the same ideas are applicable to other routing protocols. SCAN assumes a network with sufficient node density that nodes can overhear packets being received by a neighbor, in addition to packets being sent by the neighbor. SCAN nodes monitor their neighbors by

* Corresponding author Tel.:07552713334 ; fax: +0-000-000-0000
E-mail address: gul_firdose@rediffmail.com (G. F. Ahmed), raju_barskar53@rediffmail.com (R. Barskar), nepal.rgtu3@gmail.com (N. Barskar).
listening to packets that are forwarded to them. A different approach with a 2ACK scheme, which is a
network-layer technique to detect misbehaving links and to mitigate their effects, is used in [16] [17]. It
can be implemented as an add-on to existing routing protocols for MANETs, such as DSR (Dynamic
Source Routing). The 2ACK scheme detects misbehavior through the use of a new type of
acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three
nodes), in the opposite direction of the data traffic route [16]. Whereas, the proposed algorithm just uses a
simple acknowledgement approach instead a 2ACK scheme, which increases the overhead. In section IV
we are giving the comparison results for the proposed algorithm (ACK+AODV+PFC) and the 2ACK+
DSR approach, which uses an on-demand protocol DSR instead of AODV [1].

3. Mobile Ad Hoc Networks Routing Protocols

There are many ways to classify the MANET routing protocols depending on how the protocols handle
the packet to deliver from source to destination. But Routing protocols are broadly classified into three
types such as Proactive, Reactive and Hybrid protocols [4][25].

3.1 Proactive Protocols
These types of protocols are called table driven protocols in which, the route to all the nodes is
maintained in routing table. Packets are transferred over the predefined route specified in the routing
table. In this scheme, the packet forwarding is done faster but the routing overhead is greater because all
the routes have to be defined before transferring the packets. Proactive protocols have lower latency
because all the routes are maintained at all the times.
Example protocols: DSDV, OLSR (Optimized Link State Routing).

3.2 Reactive Protocols
These types of protocols are also called as On Demand Routing Protocols where the routes are not
predefined for routing. A Source node calls for the route discovery phase to determine a new route
whenever a transmission is needed. This route discovery mechanism is based on a flooding algorithm
which employs on the technique that a node just broadcasts the packet to all of its neighbors and
intermediate nodes just forward that packet to their neighbors. This is a repetitive technique until it
reaches the destination. Reactive techniques have smaller routing overheads but higher latency.
Example Protocols: DSR, AODV

3.3 Hybrid Protocols
Hybrid protocols are the combinations of reactive and proactive protocols and takes advantages of these
two protocols and as a result, routes are found quickly in the routing zone.
Example Protocol: ZRP (Zone Routing Protocol)

4. Protocol Used In MANETs

A. Ad-hoc On-demand distance vector (AODV) is another variant of classical distance vector routing
algorithm, based on DSDV and DSR .AODV (Ad Hoc On-Demand Distance Vector Routing) It is a
reactive routing protocol, meaning that it establishes a route to a destination only on demand. When the
valid route is not known by the source node, it initializes a route discovery process by broadcasting a
Route Request (RREQ) to its neighbours. Each node discards Route Requests (RREQs) it has already
seen by checking the Broadcast ID and the Sequence Number which had been included into the Route
Request (RREQ)[9].
B. DSR (Dynamic Source Routing) :-
Determining source routes require accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached with nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse.[11]

C. Zone Routing Protocol: - Zone routing protocol combines Proactive protocol features and Reactive protocol features. All nodes within hop distance at most $d$ from a node X are said to be in the routing zone of node X. All nodes at hop distance exactly $d$ is said to be peripheral nodes of node X’s routing zone. In Zone Routing Protocol Intra-zone routing involves maintaining state information for links within a short distance from any given node whereas Inter-zone routing involves using a route discovery protocol for determining routes to far away nodes[18].

5. Methodology

The brief overview of the design aspects of the algorithm with DSDV (Distance sequenced distance vector) protocol implementation, it is the simple acknowledgement approach and principle of this approach is given for conservation is discussed as follows:

Distance sequence distance vector is a proactive routing protocol, which is a conventional modification of Bellmen-Ford routing algorithm. This protocol adds sequence number, attribute for each route table in each node. A routing table is maintained at each node and this table transmits data packets to other nodes in the network. This protocol was motivated for the use of data exchange along with changing and arbitrary paths of interconnection which may not be close to any base station. All stations list available in the destinations and number of nodes required to transmit data to the destination in the routing table. The routing entry is tagged with the sequence number which is originated by the destination station. For consistency this, each station transmits and updates routing table periodically. The packets being broadcasted between stations indicate which station is sending and number of hops required to reach the particular station [18]. The data broadcast by each node will contain a new sequence number and destination address, the number of hops required to reach the destination and new sequence number, originally stamped by the destination in each new route table.

The Broadcasting of data in DSDV protocol mainly two types: 1) full dump and 2) Incremental dumps. Full dump will carry all routing information while incremental dump is only the last change of full dump. These two types of broadcasting done in the network protocol data unit. For full dumps required network protocol data unit but incremental dumps required one network protocol data unit. The proactive routing protocol is based on the periodic exchange of control message and maintaining routing table. Each node maintains complete information about the network. This information is collected from each node from the routing table. And each node knows complete topology and it can find the best node to route the information. Proactive protocols generates large volume of control message, it uses a large amount of bandwidth. The control messages may consume almost the entire bandwidth with the large amount of nodes.

In the below figure 1 each node I maintain, for each destination $x$, a set of distance $d_{ij}(x)$ for each neighbor. Node I treat the neighbor $K$ as the next hop for the packet destination for $X$, if $d_{ik}(x)$ equals minimum of all $d_{ij}(x)$ the message will be sent from I to L as the cost of path to $X$ is minimum through L [19].
The attack approach proposed in this paper structures in four successive steps (see Figure 3):

1. The Broken node (B) first launches a port scan attack [1] [7] on the destination node and finds out all the open ports.

2. Then it induces itself into the routing path between the source node and the destination by emitting protocol-compliant messages from leading both Source and Destination nodes to choose such a link for their communications [4] [9] (see Figure 4).

3. The Broken node (P) now starts altering the data packet's that are routed through it such that the Destination port number is changed to any other port that is open at the Destination node. The open ports at the Destination have already been found out by a Port Scan Attack[23] (see Figure 4).
4. The node (P) will also have to change back the port number of the acknowledgement packets to the original port number, if they are routed through the same link (hence the assumption bidirectional link).

![Diagram](https://via.placeholder.com/150)

**Algorithm:**

The general step of Improved-DSDV algorithm is described given below.

**Algorithms** – Improved-DSDV (Host S, Destination D, MAXBufferSize M, Packet A)

1. If (S. Next Hop () == UNACTIVE) then
   Use Standard DSDV;
   Else if (S. BufferLength () == FULL) then
     Discard A;
   3. If (S. BufferLength () == 0) then
     Discard A; then place at in S. Buffer;
   4. S. Broadcasts (ROUTE-REQUEST, 1, D, S);
   5. If (S. NEXT_NEIGHBOR has route to ‘D’) then
      S. RECEIVE (ROUTE_ACK)
   6. Max_Hops = 0; Min_Hop =∞; Next_Hop = 0; Updated_Time=1;
   7. Else (Host S has ROUTE_ACK Packets)
      {
      If (ROUTE_ACK. HOP_COUNT< =Max_Hops )
          {
          If (ROUTE_ACK. HOP_COUNT =Max_Hops )
            {
            If (ROUTE_ACK. UPDTD_TIME> Updated_Time)
                Host_ID = ROUTE_ACK. HOST_ID;
                Updated_Time = ROUTE_ACK. UPDTTD_TIME;
            }
          }
        }
      Else
        {
        Max_Hops = ROUTE-ACK. HOP_COUNT;
        Host_ID = ROUTE_ACK. HOST_ID;
        Updated_Time = ROUTE_ACK. UPDTTD_TIME;
        }
    }
6. Simulation Analysis and Performance Matrics

We use NS2 to simulate our proposed algorithm. In this section, the network simulation is implemented using the NS-2 simulation tool [9]. A simulation study was carried out to evaluate the performance of MANET routing protocols such as DSDV, and Improved-DSDV based on the metrics throughput, packet delivery ratio and average end-to-end delay with the following parameters:

TABLE 1: List of Simulation parameters

| Parameter                | Value                  |
|--------------------------|------------------------|
| Simulator                | NS-2                   |
| Node Movement Model      | Random                 |
| Max Speed                | 0-25m/s                |
| Traffic Type             | UDP                    |
| Bandwidth                | 1Mb/s                  |
| Transmission Range       | 250m                   |
| Packet size              | 512 bytes              |
| Area                     | 500 × 500              |
| Numbers of Nodes         | 30                     |
| Simulation Times         | 20, 40, 60, 80 & 100   |

The simulations were carried out by varying the number of nodes in multiples of 5; i.e. 5, 10, 15, 20, 25, 30 and 35. The Speed of the node is fixed. Seven Simulations were carried out for each of the three protocols. Thus a total of 21 Simulations was carried out for varying number of nodes. On similar lines, 21 Simulations were carried out by varying the speed of the nodes in multiples of 10, i.e. 10, 20, 30, 40, 50 m/S. The numbers of nodes were fixed at 30.

In order to evaluate the performance of ad hoc network routing protocols, the following metrics were considered. While comparing two protocols, we focused on two performance measurements such as Average Delay, Packet Delivery Fraction. [8]

A. Packet delivery Ratio:-
Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. A high packet delivery ratio is desired in any network.

B. Average End-to-End delay:-
The packet End-to-End delay is the average time that a packet takes to traverse the network. This is the time for the generation of the packet in the sender up to its reception at the destination’s application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, the transmission time and delays induced by routing activities and MAC control exchanges. The ratio of the number of data packets successfully delivered to the destinations to those generated by NS-2.
We evaluate mainly the performance according to the following metrics.
Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of receiving data packets.

Figure 5: Packet Delivery Ratio for DSDV, and Improved -DSDV

Figure 6: Packet delivery fraction vs. Pause time for 50-node model with 30 sources

7. Conclusion
We consider the new approach an Improved-DSDV Protocol is proposed for Ad Hoc networks. Improved-DSDV overcomes the problem of stale routes, and thereby improves the performance of regular DSDV. Simulation results show that both of the protocols deliver a greater percentage of the originated data packets when there is little node mobility, converging to 100% delivery ration when there is no node motion. The packet delivery of AODV is almost independent of the number of sources. We conclude that the AODV protocol is the ideal choice for communication. In current state problem of DSDV is routing information will maintain at each node locally in the network. All routing decisions are taken completely distribution fashion. In this state problem of DSDV is routing information will maintain at each node locally in the network. All routing decisions are taken completely distribution fashion. So the local information may be old and invalid, local information updates periodically. We compare the performance of our work with DSDV and improved DSDV. In our improved DSDV routing protocol, nodes can cooperate together to obtain an objective opinion about another node’s trustworthiness. They can also perform trusted routing behaviors according to the trust relationship among them. In future, the performance comparison can be made between the proposed protocol and the other classes of the Ad Hoc Routing Protocols with different simulation parameters and metrics.

References

[1] N Vettrivelan, Dr. A V Reddy “Performance Analysis of Three Routing Protocols for Varying MANET Size” Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol-II, IMECS 2008, 19-21 March, 2008, Hong Kong.
[2] S. Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, “A distance routing effect algorithm for mobility (dream),” in Proceedings of the IEEE/ACM international Conference on Mobile Computing and Networking (Mobicom’98), 1998, pp. 76–84.
[3] Ahmed Al-Maashri and Mohamed Ould-Khaoua. “Performance Analysis of MANET Routing Protocols in the Presence of Self-Similar Traffic”. IEEE, ISSN- 0742-1303, First published in Proc. of the 31st IEEE Conference on Local Computer Networks, 2006.
[4] Elizabeth M. Royer and C-K Toh. “A Review of current Routing Protocols for Ad-hoc Mobile Wireless Networks”, IEEE Personal Communications, Vol. 6, No.2, pp. 46-55, April 1999.
[5] C. E. Perkins and P. Bhagwat, “Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers”, in Proc. ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications, London, UK, September 1994.
[6] M. Guerrero-Zapata and N. Asokan, “Securing ad hoc routing protocols”, in Proc. 3rd ACM Workshop on Wireless Security, New York, USA, 2002.
[7] M. Guerrero-Zapata, “Secure ad hoc on-demand distance vector (SAODV) routing”, Internet Draft, IETF Mobile Ad Hoc Networking Working Group, February 2005.
[8] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A secure routing protocol for ad hoc networks”, in Proc. 10th IEEE International Conference on Network Protocols, Paris, France, November 2002.
[9] C. E. Perkins, “Ad hoc on-demand distance vector (AODV) routing”, Request For Comments (RFC) 3561, July 2003, Available online at: http://www.ietf.org/rfc/rfc3561.txt.
[10] Y. C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks”, in Proc. 8th ACM International Conference on Mobile Computing and Networking, Atlanta, USA, September 2002.
[11] D. B. Johnson, D. A Malz, and Y. C. Hu, “The dynamic source routing protocol for mobile ad hoc networks (DSR)”, Internet Draft, IETF MANET Working Group, July 2004.
[12] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “Efficient authentication and signing of multicast streams over lossy channels”, in Proc. IEEE Symposium on Security and Privacy, Berleley, USA, May 2000.
[13] S. Buchegger, and J. Le Boudec, “Performance analysis of the CONFIDANT protocol,” in Proc. 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Lausanne, Switzerland, June 2002.
[14] B. Awerbuch, D. Holmes, C. Nita-Rotaru, and H. Rubens, “An on-demand secure routing protocol resilient to Byzantine failures”, in Proc. 3rd ACM Workshop on Wireless Security, New York, USA, 2002.
[15] Y. Zhang, and W. Lee, “Intrusion detection in wireless ad-hoc networks”, in Proc. 6th ACM International Conference on Mobile Computing and Networking, Boston, USA, August 2000.
[16] Kajun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, “An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs”, IEEE Transactions on Mobile Computing, Vol-6, Issue 5, May 2007, pp. 556-550.
[17] T. V. P. Sundararajan, Dr. A. Shanmugam,” Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks”, ICGST-CNIR Journal, Volume 9, Issue 1, July 2009.
[18] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. 2002.
[19] Institute for computer science, university is garbage, Western Australian Interactive Virtual environment center (IVEC).
[20] C.E. Perkins & P. Bhagwat, “Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers”, Computer Communication Review, 24(4), 1994, 234-244.
[21] S. Murthy and J.J Garcia-Luna-Aceves, “An efficient routing protocol for wireless networks”, ACM Mobile Networks and Application Journal, Special issue on Routing in Mobile Communication Networks, 1996.
[22] [24] Payal N. Raj and Prashant B. Swedes, “DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET”, International Journal of Computer Science Issues, Vol-2, 2009.
[23] Barskar R. and Ahmed G. F, “Different Approaches on Cooperation in Wireless Ad Hoc Networks.” International Journal of Computer Applications 28(3):pp. 36-41, August 2011. Published by Foundation of Computer Science, New York, USA.
[24] Ian D. Chakeres, Elizabeth M. Belding-Royer, “AODV Routing Protocol Implementation Design”, Proceedings of the 24th International Conference on Distributed Computing Systems Workshops - W7: EC (ICDCSW’04), Vol-7, 2004, pp. 698 – 703.
[25] P. Manickam, T. Guru Baskar , M. Girija and Dr. D. Manimegalai “PERFORMANCE COMPARISONS OF ROUTING PROTOCOLS IN MOBILE AD HOC NETWORKS” International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, February 2011, pp. 98-106.