Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.126 – 132

RESEARCH ARTICLE

CACHE ENHANCEMENT IN DYNAMIC SOURCE ROUTING

Jayanti, Vikram Nandal
M.Tech student, Department of CSE, R.N College of Engineering & Management
Assistant Professor, Department of CSE, R.N College of Engineering & Management
pisces.jayanti@gmail.com, vikramcse@live.com

Abstract: On-demand routing protocols use route caches to make routing decisions. Due to mobility, cached routes easily become stale. The main problem in DSR is the bandwidth consumption due to which stale of cache occur and rerouting take place. To address the cache staleness issue, prior work in DSR used heuristics with ad hoc parameters to predict the lifetime of a link or a route. The main purpose of this paper is to provide enhanced routing protocol. In this paper, we enhance the current cache-storage mechanism by attaching some redundant information to the cached paths. This information helps to make a quicker response to some reply request and thus can reduce the average end-to-end latency further. The simulation results have proven the validity of redundant cache in reducing the average end-to-end delay and overall overhead.

Keywords- DSR, mobile ad hoc networks, cache, routing

I. INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile nodes. Mobile Ad Hoc Networking (MANET) has become an exciting and important technology in recent years because of the rapid proliferation of wireless devices. It uses radio transmission as the means for transmitting data. Routing protocols for ad hoc networks can be classified into two major types: proactive and on-demand. Proactive protocols attempt to maintain up-to-date routing information to all nodes by periodically disseminating topology updates throughout the network. In contrast, on demand protocols attempt to discover a route only when a route is needed. To reduce the overhead and the latency of initiating a route discovery for each packet, on-demand routing protocols use route Caches. Due to mobility, cached routes easily become stale. Routing protocols in conventional wired networks generally use either distance vector or link state routing algorithms, both of which require periodic routing advertisements to be broadcast by each router.

The rest of this paper is organized as follows: Section II summarizes related researches. Section III gives a brief introduction of the DSR protocol. Section IV describes our Enhanced cache in detail. Section V describes Experimental results and analysis. In Section VI, we draw conclusion and give future work.

II. RELATED WORK

Haas, et al [1] proposed a protocol (SRP) that can be applied to several existing routing protocols. SRP requires that, for every route discovery, source and destination must have a security association between them. It also requires clock synchronization. S. Buchegger et al [2] proposed CONFIDANT routing protocol extension over DSR to provide security. In this paper we review secure routing protocols based on DSR. An active network approach by Yu He et al [3] proposed algorithm for improving route failures and overhead with DSR. This method uses an active packet that periodically visits all nodes it can reach to get network topology information existing routes, but also cache future routes based on the topology information. Thus both route request flooding for the stale routes and new routes are reduced. The reduction in the flooding rate also significantly reduces the routing overhead and then uses this information to validate and update the cached routes. With active networking, they not only adjust existing routes, but also cache future routes based on the topology information. Thus both route request flooding for the stale routes and new routes are reduced. The reduction in the flooding rate also significantly reduces the routing overhead. K. Sanzgiri et al [4] proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN, every node that forwards a route discovery or a route reply message must also sign it, (which is very computing power consuming and causes the size of the routing messages to increase at each hop), whereas the proposal presented in this paper only require originators to sign the message. Hubaux et al [5] proposed a method that is designed to ensure equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates. Kong, et al. [6] have proposed a secure ad hoc routing protocol based on secret sharing; unfortunately, this protocol is based on erroneous assumptions, e.g., that each node cannot impersonate the MAC address of multiple other nodes. Yi, et al. [5] also have proposed a general framework for secure ad hoc routing called the SAR. Zhou et al[7] primarily discuss key management. They devote a section to secure routing, but essentially conclude that “nodes can protect routing information in the same way they protect data traffic”. They also observe that denial-of-service attacks against routing will be treated as damage and routed around.

III. DYNAMIC SOURCE ROUTING

Dynamic source routing protocol (DSR) is an on-demand protocol based on source routing designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference is that it is beacon-less and hence does not require periodic hello packet (beacon) transmissions. In DSR every mobile node in the network needs to maintain a route cache where it caches source routes that it has learned. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding Route Request packets in the network. DSR protocol is based on two mechanisms: Route Discovery and Route Maintenance.

Route Discovery: DSR uses this process to find the route and to transmit the data from a source to destination where the source node is unaware of the destination route.

Route Maintenance: Route maintenance can be achieved by two different process:-

i). Hop-by-hop acknowledgement at the data link layer allows an early and retransmission of lost or corrupt packets.

ii). End-to-end acknowledgement may be used if wireless transmission between two hosts does not work equally well in both directions.

Basic DSR Algorithm:

The DSR protocol allows nodes to dynamically discover a *source route* across multiple network hops to any destination in the ad hoc network. DSR routing algorithm for Route Request and Message Transfer

```
Route Request and Message Transfer
➢ Find the Route path from Source to Destination Node
➢ If the Path exists then
    ▪ Check the status of the Destination Node status
    ▪ If the Status is True
        ❖ Send the Packets to the Destination Node
        ❖ Count the No of Packets
        ❖ Receive the Acknowledgements
        ❖ Update the Packets Information in the Cache Table
➢ Else
    ▪ Send the Route Request to the Neighboring Nodes
    ▪ Receive the Route Request
    ▪ If Path is Available and Status of the Node is True
        ❖ Send the Send the Route Reply to the Requested Node
    ▪ Else
        ❖ Forward the Route Request to the Neighboring Nodes
        ❖ Receive the Route Reply
        ❖ Add the Node name along with the Path
        ❖ Send back the Route Reply to the Requested Node
        ❖ Add the Path in the Cache Table
```

On the basis of this algorithm, this paper proposes enhanced cache algorithm of DSR for formal verification in the following section because of following flaws in DSR protocol:

- Bandwidth consumes by nodes can easily corrupt the system through any node exists in the network.
- The Stale routes cause packet losses if packets cannot be salvaged by intermediate nodes.
- DSR fails to protect the destination from malicious nodes. Any node that exists in same network can easily corrupt other nodes.

IV. CACHE ENHANCEMENT IN DSR

In a mobile ad hoc network, nodes move arbitrarily. Mobility presents a fundamental challenge to routing protocols. On demand protocols attempt to discover a route only when a route is needed. To reduce the overhead and the latency of initiating a route discovery for each packet, on-demand routing protocols use route Caches. Due to mobility, cached routes easily become stale. Using stale routes causes packet losses, and increases latency and overhead. This section investigates how to make on-demand routing Protocols adapt quickly to topology changes.

We have designed a distributed algorithm that uses the information kept by each node to achieve distributed cache updating. When a link failure or node failure is detected, the algorithm notifies selected neighborhood nodes about the broken link: the closest upstream and/or downstream nodes on each route containing the broken link, and the neighbors that learned the link through ROUTE REPLIES. When a node receives a notification, the algorithm notifies selected neighbors. Thus, the broken link information will be quickly propagated to all reachable nodes that need to be notified.

The algorithm has the following desirable properties:

Distributed: The algorithm uses only local information and communicates with neighborhood Nodes; therefore, it is scalable with network size.

Adaptive: The algorithm notifies only the nodes that have cached a broken link to update their Caches; therefore, cache update overhead is minimized.

On-demand: cache updating is triggered on-demand, without periodic behavior.

Enhance DSR Algorithm:

1. *Call RootDiscovery(S, D)*
2. *Identification of malicious node*

   Each mobile host delay slightly before replying from its cache

   a. *Pick a delay period d = H × (h-1 + r)*

      H : small constant delay,

      h: number of hops for the route to be returned in this host's reply,

      r : random number (0~1)

   b. *Delay transmitting the route reply from this host for a period of d*
   c. *If a packet is received by this host during the beyond delay period and the length of the route on this packet is less than h,*
   d. *Call DSR Failure-NodeDetection(I)*
3. *DSR Cache-Update Algorithm(I0)*

1. Algorithm for RootDiscovery(S,J, D)

```
/* S is the node that want to transfer data to the
destination node D. J is the intermediate node*/
{
if(S=D)
{
Return "Success"
}
Else
{
Node S will broadcast the message to all
surrounding nodes and get Response time and Load
Find Node with Minimum Load and Minimum
Cost called Node J
if(Reply_Status(J)=true)
{
set J=CureentNode
RootDiscovery(J,D)
}}
```

2. Algorithm for DSR FailureNodeDetection(I):

```
DSR Failure-NodeDetection(I)
/* I is the Node over the network*/
{
A node will send a packet to Node I with
defined hop time and wait for the
acknowledgement.
if (Check(REPLY)!=NULL)
{
if(ReplyTime(I0)<HopTime)
{
Return True;
}
else
{
Return False;
}}
else
{
return Failure Node;
}}
if(CheckForward(Message)=true)
{
return true;
}
else
return failure;
}
```

3. Algorithm for DSRCache-Update (I, J)

```
/* Node I is detected as the malicious node and node J is the node that detect the failure node I.
{
As the Failure Node Detected by Node J0 it will perform a request to block this node and perform the Cache Updatation.
It set the Reply status of NodeI= FALSE it seems all neighboringnodes not to use this node as part of network
}
```

Node misbehaves when node does not send the packets within Hop Time. If node is not behaving correctly, then it means it has the packet delivery ratio less than 98 % and those nodes will be blocked temporarily. Its neighboring node informs to reply the nodes about blocked node and the cache table is updated.

Figure 1 shows the routing of message from source to destination from different intermediate nodes. In this the node 4 is malicious. If any packet transmitted through this link or this node, so that other nodes may not corrupt and cache table is updated according to new status. So according to this Figure 1, node 4 will not participate in routing. So Figure 1 shows that the other nodes will not get affected and secure transmission takes place.

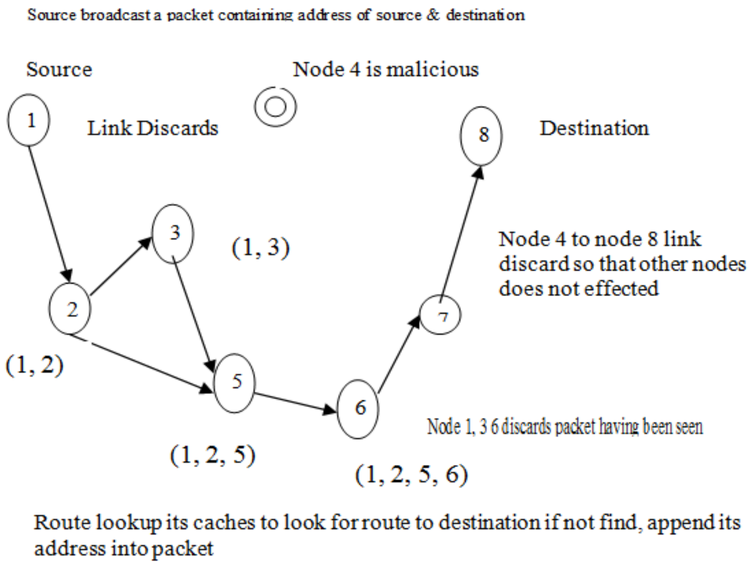
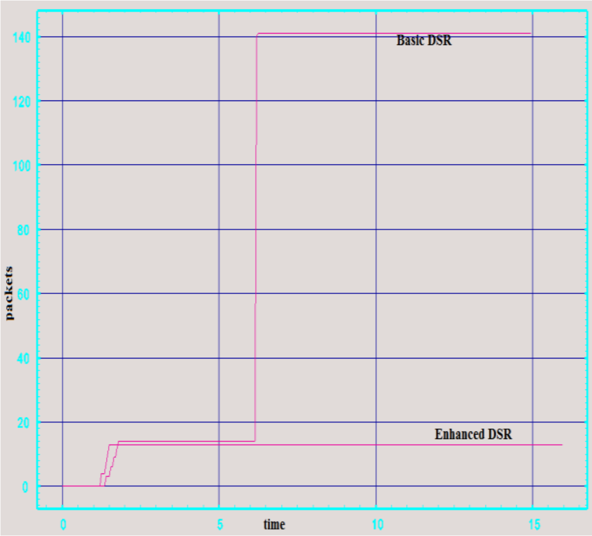

Source broadcast a packet containing address of source & destination
Source
Node 4 is malicious
1
Link Discards
8
Destination
3
(1, 3)
Node 4 to node 8 link discard so that other nodes does not effected
2
7
(1, 2)
5
6
Node 1, 3 6 discards packet having been seen
(1, 2, 5)
(1, 2, 5, 6)
Route lookup its caches to look for route to destination if not find, append its address into packet

Fig1. Message Transfer in Enhance Cache in DSR

V. RESULTS

Proposed approach is implemented using Network Simulator (NS2). This paper presents updates route caches in an adaptive manner. It defines a new cache structure called a cache table to maintain the information necessary for cache updates. It presents an Enhance cache in DSR algorithm that uses the local information kept by each node to notify all reachable nodes that have cached a broken link or node failure due to malicious node. Network is simulated for varying no. of nodes and results are obtained in terms of no. of packets lost and no. of packets received. Following graph results are showing results for 50 nodes and it can be seen that if we are using Enhance

DSR system then the packet lost is low as compared to basic DSR. Also there is much increase in received packet ratio in case of enhanced DSR system.



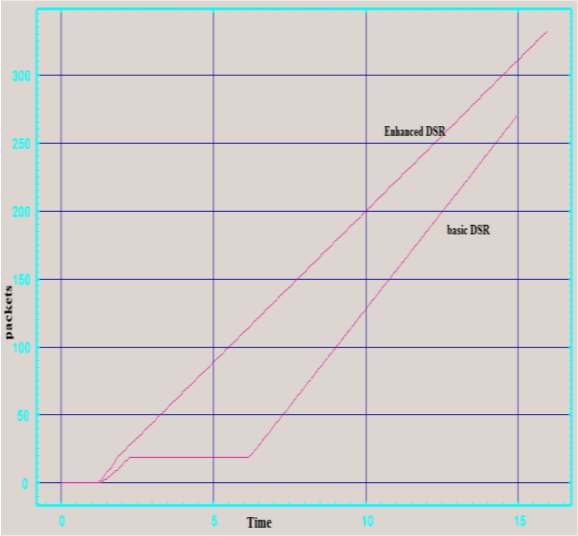


Fig 2 Packet Lost with Basic DSR and Enhance DSR Fig 3 Packet Received with Basic DSR and Enhance DSR

VI. CONCLUSION

The algorithm presented in this paper for Identification of malicious node is used to find out the malicious node. We defined a new cache structure called a cache table to maintain the information necessary for cache updates. In this paper a cache update algorithm is presented that uses the local information kept by each node to notify all reachable nodes that have cached a broken link. Simulation study shows that Enhancement of Cache in DSR works better than DSR when malicious node is found. Our solution is also applicable to other on-demand routing protocols. It concludes that cache updating is a key to the adaptation of on-demand routing protocols to mobility.

REFERENCES

[1]P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan 2002.

[2]S. Buchegger, and J.-Y. Le Boudec, “Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad hoc NeTworks),” Proc. 3rd Symp. Mobile Ad hoc Networking and Computing (MobiHoc 2002), ACM Press, 2002, pp. 226-236.

[3]Yu He , Cauligi S. Raghavendra, Active Packets Improve Dynamic Source Routing for Ad-hoc Networks.

[4]K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, “A Secure Routing Protocol for Ad hoc Networks”, Proc. 10th IEEE Int’l. Conf. Network Protocols (ICNP’02), IEEE Press, 2002, pp. 78-87.

[5]J.-P. HuBaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In Proc. ACM MOBICOM, Oct. 2001.

[6]J. Kong et al. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proc. IEEE ICNP, pages 251–260, 2001.

[7] L. Zhou and Z. J. Haas. Securing ad hoc networks. IEEE Network Magazine, 13(6):24–30, November/December 1999.

[8] Dr. Yudhvir Singh, Aarti, “Review of scalability and mobility effect on the TCP performance in MANET”, National Conference on Emgerging Trends in Engg. & Tech., India, pp339-342.

[9] L. R. Ford Jr. and D. R. Fulkerson, Flows in Networks, Princeton Univ. Press, 1962 [24]

[10] S. Murthy and J. J. Garcia-Luna-Aceves, “An Efficient Routing Protocol for Wireless Networks,” ACM Mobile Networks and App. J., Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183–97.
[11] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad-Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer, 1996, pp. 153 81.
[12] Elizabeth M. Royer and Chai-Keong Toh, “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”, IEEE Personal Communications Magazine, April 1999, pages 46-55.