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. 2, Issue. 12, December 2013, pg.15 – 20

SURVEY ARTICLE

Survey on Attacks in Routing Protocols In Mobile Ad-Hoc Network

Jignesh B. Maheta[1], Harikrishna Jethva[2], Bhadreshsinh G. Gohil[3]

[1](PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University, Ahmedabad
Email: jigs007d2d@gmail.com)
[2] (Associate Professor, L D Engineering College, Ahmedabad
Email: hbjethva@gmail.com)
[3] (Assistant Professor, SIEM, Rajpur, Mehsana
E-mail: bhadu.gohil@gmail.com)

***Abstract*— Nowadays, Mobile Ad-Hoc Network is very important Technology because it has rapid roliferations of wireless devices. These networks are highly vulnerable to attacks because of the open medium, dynamically changing topology. It has ability to manage the network independently. So a node can misbehave and network may fail to establish route the routing protocols using UDP traffic have been done by considering various parameters such as mobility, network load and pause time. The purpose of this work is to understand there working mechanism and investigate that which routing protocol gives better Performance data due to its malicious activity. In this work I will analyse how the DSR, AODV and TORA routing protocols work in MANET and Attacks on Routing Protocols.**

Keywords- Routing Protocols in MANET; AODV; DSR; TORA; Attacks in Routing Protocols

I. Introduction

1.1 Mobile Ad-Hoc Network

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes which can freely and dynamically self-organize and co-operative in to arbitrary and temporary network topologies, allowing peoples and devices to communicate without any pre-existing communication architecture [1][2]. Each node in the ad hoc network acts as a router, forwarding data packets for other nodes. A central challenge in the design of mobile ad hoc networks is the development of routing protocols that can efficiently find the transmission paths between two communicating nodes. The ad hoc networks are very flexible and suitable for several types of applications due to its feature like they allow the establishment of temporary communication without any pre-installed infrastructure. With newly emerging radio technologies, e.g. IEEE 802.11and Bluetooth, the realization of multimedia applications over mobile ad-hoc networks becomes more realistic. Our goal is to carry out a systematic performance study of an on demand routing protocol AODV, DSR and TORA [1] [2] for ad hoc networks. Generally the network protocols were simulated as a function of pause time (node mobility), but not as a function of network size.

II. Literature Review

2.1 Routing Protocols in Mobile Ad-Hoc Network

The routing protocols for MANET 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 consistent and up-to-date routing information to all nodes is maintained at each node whereas in on-demand routing the routes are created only when desired by the source host.[1][8]

Here we discuss the 3 on demand routing protocols –AODV, DSR and TORA.

2.1.1 AODV ROUTING PROTOCOL DESCRIPTION:

Ad hoc On Demand Distance Vector (AODV) is a reactive routing protocol which initiates a route discovery process only when it has data packets to transmit and it does not have any route path towards the destination node, that is, route discovery in AODV is called as on-demand.[9] AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to avoid the routing loops that may occur during the routing calculation process. All routing packets carry these sequence numbers.

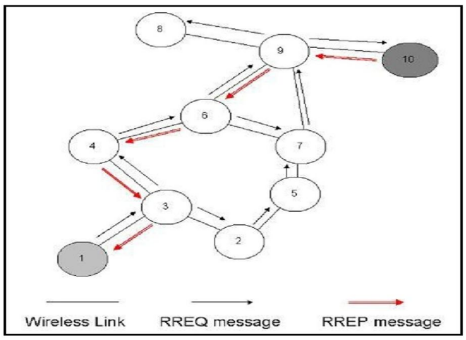


Figure 2.1 AODV Route Discovery Process

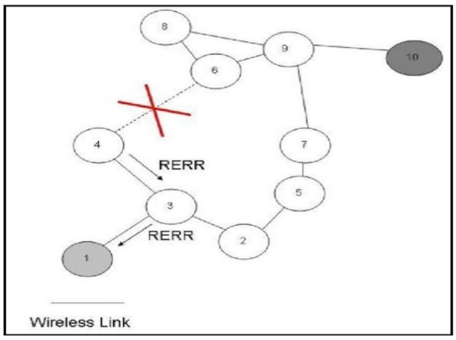


Figure 2.2 AODV Route Error message generation

Route Discovery Process:

During a route discovery process, the source node broadcasts a route query packet to its neighbors. If any of the neighbors has a route to the destination, it replies to the query with a route reply packet; otherwise, the neighbors rebroadcast the route query packet. Finally, some query packets reach to the destination.Figure 2.1 shows the route discovery process from source node1 to destination node 10. At that time, a reply packet is produced and transmitted tracing back the route traversed by the query packet as shown in Figure 2.1.

AODV Route Message Generation:

The route maintenance process in AODV is very simple. When the link in the communication path between node 1 and node 10 breaks the upstream node that is affected by the break, in this case node 4 generates and broadcasts a RERR message. The RERR message eventually ends up in source node 1. After receiving the RERR message, node 1 will generate a new RREQ message (Figure 2.2).

AODV Route Maintenance Process

Finally, if node 2 already has a route to node 10, it will generate a RREP message, as indicated in Figure 2.3. Otherwise, it will re-broadcast the RREQ from source node 1 to destination node 10 as shown in Figure 2.3.

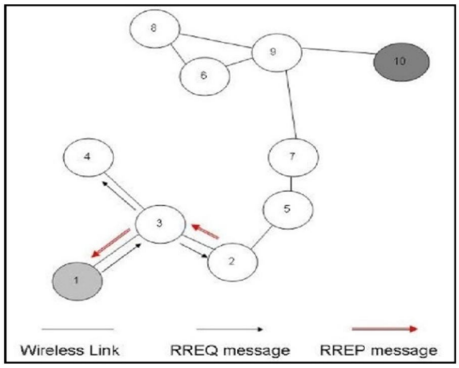


Figure 2.3. *AODV Route Maintenance Process*

2.1.2 DSR Routing Protocol Description

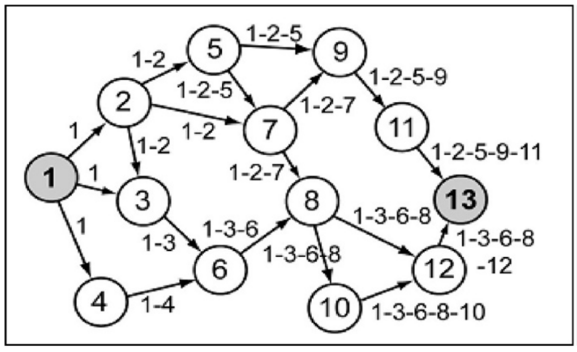
The Dynamic Source Routing (DSR) protocol is a reactive routing protocol based on source routing. In the source routing, a source determines the perfect sequence of nodes with which it propagate a packet towards the destination. The list of intermediate nodes for routing is explicitly stored in the packet's header [6].

In DSR, every mobile node needs to maintain a route cache where it caches source routes. When a source node wants to send a packet to some other intermediate node, it first checks its route cache for a source route to the destination for successful delivery of data packets. In this case if a route is found, the source node uses this route to propagate the data packet otherwise it initiates the route discovery process. Route discovery and route maintenance are the two main features of the DSR protocol [9].

Route Discovery

For route discovery, the source node starts by broadcasting a route request packet that can be received by all neighbour nodes within its wireless transmission range. The route request contains the address of the destination host, referred to as the target of the route discovery, the source's address, a route record field and a unique identification number (Figure 2.4). At the end, the source node should receive a route reply packet with a list of network nodes through which it should transmit the data packets that is supposed the route discovery process was successful [3].

During the route discovery process, the route record field is used to contain the sequence of hops which already taken. At start, all senders initiate the route record as a list with a single node containing itself. The next intermediate node attaches itself to the list and so on. Each route request packet also contains a unique identification number called as request_id which is a simple counter increased whenever a new route request packet is being sent by the source node. So each route request packet can be uniquely identified through its initiator's address and request_id. When a node receives a route request packet, it is important to process the request in the following given order. This way we can make sure that no loops will occur during the broadcasting of the packets.



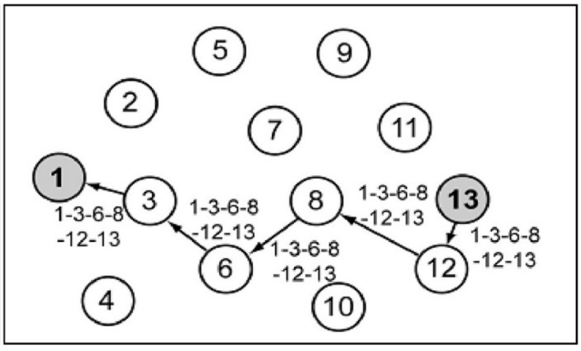


Figure 2.4 Building of the record during route discovery **Figure 2.5** Propagation of the route reply

- ✓ If the pair < source node address, request_id > is found in the list of recent route requests, the packet is discarded.

- ✓ If the host's address is already listed in the request's route record, the packet is also discarded. This indicates removal same request that arrive by using a loop.
- ✓ If the destination address in the route request matches the host's address, the route record field contains the route by which the request reached this host from the source node. A route reply packet is sent back to the source node with a copy of this route. Otherwise, add this node's address to the route record field and re-broadcast this packet.

A route reply is sent back either if the request packet reaches the destination node itself, or if the request reaches an intermediate node which has an active route to the destination in its route cache. The route record field in the request packet indicates the sequence of hops which was considered. If the destination node generating the route replies, it just takes the route record field of the route request and puts it into the route reply. If the responding node is an intermediate node, it attaches the cached route to the route record and then generates the route reply (Figure 2.5).Sending back route replies can be processed with two different ways: DSR may use symmetric links. In the case of symmetric links, the node generating the route reply just uses the reverse route of the route record. When using asymmetric links, the node needs to initiate its own route discovery process and back the route reply on the new route request.

Route Maintenance:

Route maintenance can be accomplished by two different processes:

1.Hop-by-hop acknowledgement

2.End-to-end acknowledgements

Hop-by-hop acknowledgement is the process at the data link layer which allows an early detection and re-transmission of lost packets. If the data link layer determines a fatal transmission error, a route error packet is being sent back to the sender of the packet. The route error packet contains the information about the address of the node detecting the error and the host's address which was trying to transmit the packet. Whenever a node receives a route error packet, the hop is removed from the route cache and all routes containing this hop are truncated at that point.When wireless transmission between two hosts does not process equally well in both directions, end-to-end acknowledgement may be used. As long as a route exists, the two end nodes are able to communicate and route maintenance is possible. In this case, acknowledgements or replies on the transport layer used to indicate the status of the route from one host to the another. However, with end-to-end acknowledgement it is not possible to find out the hop which has been in error.

2.1.3 TORA ROUTING PROTOCOL DESCRIPTION:

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal. TORA is proposed for highly dynamic mobile, multi-hop wireless networks. It is a source-initiated on-demand routing protocol [12]. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes.

The protocol has three basic functions: *Route Creation* and *Route maintenance*. TORA can suffer from unbounded worst-case convergence time for very stressful scenarios. TORA has a unique feature of maintaining multiple routes to the destination so that topological changes do not require any reaction at all. The protocol reacts only when all routes to the destination are lost. In the event of network partitions the protocol is able to detect the partition and erase all invalid routes.

2.2 ATTACKS IN MOBILE AD HOC NETWORKS

There are numerous types of attacks occur in ad hoc network, but are mainly classified into two types, external attacks and internal attacks. In external attack, the attacker aims to cause congestion propagate fake routing information or disturb nodes from providing services. In internal attack the adversary wants to gain normal access to the network activities, either by some impersonation to get the access to network as the new node, or by directly compromising a current node and using it as basis to conduct its malicious behaviour [6][13][14].

TYPES OF ATTACKS:

Collision Attack: Deliberates collisions or corruption induced by an attacker in order to deny the use of a link.

Impersonation Attack: The attacker nodes impersonates a legitimate node and joins the network undetectable, sends false routing information, masked as some other trusted node.

Black Hole Attack: In this attack, the attacker node injects false route replies to the route requests claiming to have the shortest path to the destination node whose packets it wants to intercept. Once the fictitious route has been established the active route is routed through the attacker node. The attacker node is then in a position to misuse or discard any or all of the network traffic being routed through it.

Wormhole attack: Adversaries cooperate to provide a low-latency side- channel for communication by means of a second radio with higher-power and long-range link. The wormhole attack involves the cooperation between two attacking nodes. One attacker captures routing traffic at one point of the network and tunnels it to another point in the network that shares a private high speed communication link between the attackers, and then selectively injects tunnel traffic back into the network. The two colluding attacker can potentially distort the topology and establish routes under the control over the wormhole link.

Denial of Service: Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

Flooding Attack: Overwhelms victim's limited resources: memory, processing or bandwidth.

2.3 Attacks Against Routing:

Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviours. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path. Attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack.

There are some attacks against routing that have been studied:

- Impersonating another node to spoof route message.
- Advertising a false route metric to misrepresent the topology.
- Sending a route message with wrong sequence number to suppress other legitimate route messages.
- Flooding Route Discover excessively as a DoS attack.
- Modifying a Route Reply message to inject a false route.
- Generating bogus Route Error to disrupt a working route.
- Suppressing Route Error to mislead others.

III. CONCLUSION

We can summarize our final conclusion from our analysis as AODV has the best all round performance.DSR is suitable for networks with moderate mobility rate. It has low overhead that makes it suitable for low bandwidth and low power network. TORA is suitable for operation in large mobile networks having dense population of nodes. The major benefit is its excellent support for multiple routes and multicasting. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path.

References

[1] D. Dhakal and K. Gautam, "Performance Comparison of AODV and DSR Routing Protocols in Mobile Ad-hoc Networks : A Survey," vol. 2, no. 3, pp. 258–265, 2013.

[2] K. Prateek, "MANET-Evaluation of DSDV, AODV and DSR Routing Protocol," vol. 2, no. 1, pp. 99–104, 2013.

[3] C. Faculty, "Analysis And Evaluation Optimization Dynamic Source Routing (DSR) Protocol in Mobile Adhoc Network Based on Ant Algorithm," pp. 400–404, 2013.

[4] L. M. T. Harb, "PERFORMANCE OF MOBILE AD HOC," 2013.

[5] "A SURVEY OF ROUTING PROTOCOLS AND GEOGRAPHIC ROUTING," vol. 3, no. 12, pp. 51–56, 2012.

[6] R. Aggarwal, "Security on Dynamic Source Routing Protocol Using Onion Routing Encryption," no. 6, pp. 42–46, 2013.

[7] Gopinath G. and Jayakumar Geetha ," Ad Hoc Mobile Wireless Networks Routing Protocols – A Review", Journal of Computer Science 3 (8): 574-582, 2007 ISSN 1549-3636.

[8] Yadav R.P. and Yadav Narendra Singh, "Performance Comparison and Analysis of Table - Driven and On-Demand Routing Protocols for Mobile Ad-hoc Networks", International Journal of Information Technology Volume 4 Number 2.

[9] Lee Sung Ju and Toh Chai Keong, "A Simulation Study of Table Driven and On-Demand Ad-hoc Routing Protocols ", IEEE Network

[10] Charles E. Perkins, Ad Hoc Networking, Addison-Wesley, March 2005.

[11] Samir R. Das, Charles E. Perkins, Elizabeth E. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks".

[12] Gupta K. Anuj, Sadawarti Harsh and Verma K. Anil, "Performance analysis of AODV, DSR & TORA Routing Protocols" , IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010 ISSN: 1793-8236

[13] P. N. Patil, "Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching," 2013.

[14] M. S. Amutha, "Secure Implementation Of Routing Protocols For Wireless Ad Hoc Networks."

