IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 8, Issue 1 (Nov-Dec. 2012), PP 34-40
www.iosrjournals.org

Survey of Routing Protocols for Mobile Ad hoc Networks

Ashima Batra[1], Abhishek Shukla[2], Sanjeev Thakur[3], Rana Majumdar[4]
[1]*Department of Computer Science & Engineering, Shri Balwant Institute of Technology, Sonepat, Haryana, India*
[2]*Department of Computer Science & Engineering, Axis College of Technology and Management, Kanpur, U.P., India*
[3]*Department of Computer Science & Engineering, Amity Institute of Computer Science, Noida, U.P., India*
[4]*Department of Computer Science & Engineering, Amity School of Engineering and Technology, Noida, U.P., India*

Abstract: *In this paper we represent a survey of various existing secure routing protocols for MANET's. A mobile ad hoc network is a self configuring mobile nodes network. Significant progress has been made for making mobile ad hoc network secure and dynamic. Its infrastructure less and absence of any centralized authority makes these networks more vulnerable to security attacks. Due to these security threats, there is need for development of algorithm and protocols for a secured ad hoc network. In this paper a comparative study of different routing protocols is discussed as Ad Hoc on Demand Distance Vector routing (AODV), Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA) security threats within MANET network.*

Keywords: MANET's; Denial of Services; DSR; AODV; TORA

I. Introduction

In wireless ad hoc network there is no pre-deployed infrastructure for routing packets end to end and instead of this there are mobile nodes communicating via radio links that can temporarily form a network.

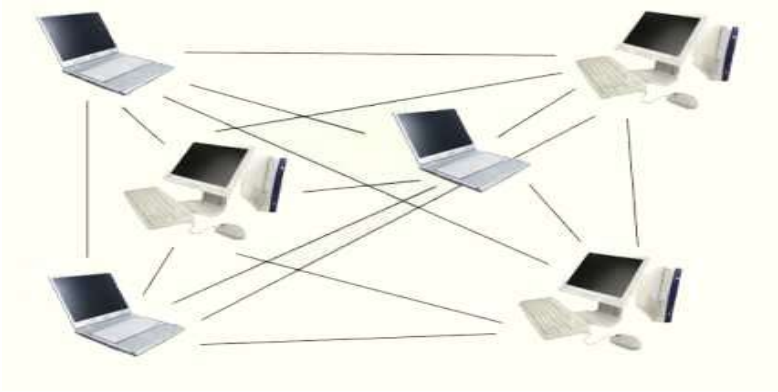

Fig. 1 Mobile Ad Hoc Network

The topology is highly dynamic and the nodes have a limited transmission range, so each node needs the assistance of its neighboring node for packet forwarding. The information is exchanged and updated dynamically from time to time. But on demand routing protocol instead of generating periodical updates, find the route to the destination node only when the source node have a data packet to be sent to the destination node. [1]
Therefore security in ad hoc is a challenge for basic network operations like packet forwarding and routing .In this paper we expose various security threats and find the way to route packet securely.
This paper deals with various issues that lack in mobile ad hoc network and then with various protocols associated with routing in MANET's.

II. Lack Of Security In Ad Hoc Network

MANET's does not have fixed infrastructure therefore all the network details are obtained on fly and so are susceptible to the wireless network attacks. [2]

A. *Lack of Secure Boundaries*

In mobile ad hoc network nodes are free to join, move and leave the network according to their need in the wired network, nodes must get physical access to the network medium, or even pass through several firewall

and gateway before their behavior become malicious to the targets. However, in MANET's, there is no need for physical access to visit the network: once the node is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes. As a result MANET's does not provide secure boundaries.

B. ***Threats from Compromised nodes Inside the Network***

Because of the mobility of the ad hoc network, a compromised node cannot be easily determined, that node frequently change its attack target and perform malicious behavior in the network, thus it is very difficult to track the malicious behavior performed by a compromised node. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

C. ***Lack of Centralized Management Facility***

It is not easy to monitor traffic in a highly dynamic network because of absence of any centralized monitoring. Therefore failures like packet dropping, path breakage are common. These malicious failures are more difficult to detect, especially when topology changes frequently and their attack target also changes in different periods of time. However, we can easily find from a system point of view that the node has performed such a large amount of misbehaviors that we can safely conclude that all of the failures caused by this node should be malicious failure, though these failures occur in different nodes at different time.

D. ***Restricted Power Supply***

Mobile ad hoc network mainly work on battery power, some time the nodes become selfish as they have limited battery power due to this selfishness some problems are caused, when there is a need for this node to cooperate with other nodes to support some functions in the network. As an example consider a cluster-based intrusion detection technique. In this, there is no need that every node in the ad hoc network is the monitoring node all the time; instead, a cluster of neighboring MANET nodes can randomly elect a monitoring node that will observe the abnormal behaviors in the network traffic for the entire cluster. However, an important precondition for the success of this technique is that every node in the cluster is willing to take their responsibility as a monitoring node and serve for all other nodes in a period of time. There may be some nodes that behave selfishly and do not want to cooperate in the monitoring node election process, which will make the election fail if there are too many selfish nodes.

E. ***Scalability***

In a traditional wired network no of node connected does not change frequently so its scale is generally predefined but in ad hoc network nodes are mobile numbers of nodes connected in network changes frequently so its scale keeps on changing frequently. As a results its protocols and services such as key management, routing protocols should be compatible to this change. [3]

III. Protocols In MANET's

Routing is a term that defines the route from source node to destination node. Routing in MANETs is more difficult than routing in wired networks. In MANETs there are two types of routing: Table-driven routing and On-demand routing.

Table-driven ad hoc routing protocols maintain the routing information of each and every node connected to all other nodes in the network. Also known as *proactive*, these protocols allow every node to have a clear and consistent view of the network topology by transmitting updating messages periodically. Another approach is the source-initiated on-demand routing. According to this approach, a route is created only when the source node requires a route to a specific destination. A route is obtained by initiating the route discovery procedure by the source node. While route discovery, the data packets transmitted are buffered and are sent when the path is established. An established route is maintained as long as it is required through a *route maintenance* procedure. There is no routing protocol which is perfect for all kinds of MANETs.

Each routing protocol has its own strengths in some specific networking environments, but mobile nodes should be able to operate in every environment. A challenge is how to achieve security in routing as high as possible when it crosses over different environments

A. ***DSR (Dynamic Source Routing)***

Dynamic source routing belongs to the class of reactive routing protocols which is based on the theory of source-based routing rather than table-based. This protocol is source-initiated rather than hop-by-hop. This is particularly designed for use in multi hop wireless ad hoc networks of mobile nodes. It allows a node to

dynamically discover a route having multiple hops to any destination. Each packet in its header carries a complete ordered list of nodes through which the packet must pass. [5]

1) Route Discovery:

When a node wants to send a packet to a destination, it checks the source route to the destination in its cache. If no route is found in its cache, it requests a route by broadcasting Route request Packet (RREQ) broadcast. This packet includes the destination address, the source address and an identification number (request id). Each node receiving the RREQ, looks for the destination in its cache. If it does not know the route to the destination, it adds its address to the 'route record' in the RREQ and propagates it by transmitting it as a local broadcast packet (with the same request id). To limit the number of RREQ's, if one node receiving the RREQ has recently seen another RREQ from the same source, with the same request id, or if it finds its own address in the route record, then it discards the RREQ. RREP (Route Reply) is sent when the RREQ reaches the destination or an intermediate node that has the route to the destination. When the RREQ reaches the destination, it has the route record with the sequence of nodes crossed. If the node that generates the RREP is the destination, then it copies the route record sent in the RREQ. If the node that generates the RREP is an intermediate node, then it adds to the route record sent the route to the destination stored by it. If the links are bidirectional the RREP is sent by the reverse path. If the links are not symmetric, the node that sends the RREP must update its previous stored entry to the source (or to begin a route discovery to the source).

2) Route Maintenance:

Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledgment messages are used to verify the correct operation of the route links. In wireless networks acknowledgments are often provided as e.g. an existing standard part of the MAC protocol in use, such as the link layer acknowledgment frame defined by IEEE 802.11. If a built-in acknowledgment mechanism is not available, the node transmitting the message can explicitly request a DSR specific software acknowledgment to be returned by the next node along the route. When problem detected, send *Route Error* packet to original sender to perform new route discovery

- Host detects the error and the host it was attempting.
- Route Error is sent back to the sender the packet – original source.

Advantages

- Its first advantage is the small overload in terms of packets to obtain routes, since DSR only manages the routes between nodes who want to communicate. Besides, DSR uses caching, and that can reduce the load of future route discovery.
- Another advantage is that only one RREQ process can produce some routes to the destination, thanks to the responses of the caches of intermediate nodes. If we compare the following protocols: DSDV, OLSR, AODV and DSR, the last one is the only who has numerous paths.
- Besides, there are no periodical updates.

Disadvantages

- However, DSR has disadvantages too. Using DSR, when a source sends a packet to any destination, the route is within the header. It is obvious that we are introducing byte overhead if the number of nodes is big in the network.
- Another disadvantage is the flooding. It can reach all the nodes in the network, when it is unnecessary. Besides, we have to prevent the collisions produced by the RREQ broadcasts (we can introduce random delays before sending the RREQ).
- The cache using also creates a problem: An intermediate node can corrupt the other nodes cache sending RREP using an obsolete cache. Therefore, we do not know how often the caches must be updated. If we update the cache very often, we produce overload on the network. But if we rarely update the cache, if the nodes move fast, we will have a wrong route
- Broken links cannot be repaired locally.
- It performs badly at high mobility because of the caching.

B. *AODV (Ad Hoc on Demand Distance Vector)*

AODV is a variation of Destination-Sequenced Distance-Vector (DSDV) routing protocol which is collectively based on DSDV and DSR. It aims to minimize the requirement of system-wide broadcasts to its extreme. It does not maintain routes from every node to every other node in the network rather they are

discovered as and when needed & are maintained only as long as they are required. The key steps of algorithm used by AODV for establishment of unicast routes are explained below. [4]

1) Route Discovery:

When a node wants to send a data packet to a destination node, the entries in route table are checked to ensure whether there is a current route to that destination node or not. If it is there, the data packet is forwarded to the appropriate next hop toward the destination. If it is not there, the route discovery process is initiated. AODV initiates a route discovery process using Route Request (RREQ) and Route Reply (RREP). The source node will create a RREQ packet containing its IP address, its current sequence number, the destination's IP address, the destination's last sequence number and broadcast ID. The broadcast ID is incremented each time the source node initiates RREQ. Basically, the sequence numbers are used to determine the timeliness of each data packet and the broadcast ID & the IP address together form a unique identifier for RREQ so as to uniquely identify each request. The requests are sent using RREQ message and the information in connection with creation of a route is sent back in RREP message. The source node broadcasts the RREQ packet to its neighbors and then sets a timer to wait for a reply. To process the RREQ, the node sets up a reverse route entry for the source node in its route table. This helps to know how to forward a RREP to the source. Basically a lifetime is associated with the reverse route entry and if this entry is not used within this lifetime, the route information is deleted. If the RREQ is lost during transmission, the source node is allowed to broadcast again using route discovery mechanism.

2) Route Maintenance:

A route discovered between a source node and destination node is maintained as long as needed by the source node. Since there is movement of nodes in mobile ad-hoc network and if the source node moves during an active session, it can reinitiate route discovery mechanism to establish a new route to destination. Conversely, if the destination node or some intermediate node moves, the node upstream of the break initiates Route Error (RERR) message to the affected active upstream neighbors/nodes. Consequently, these nodes propagate the RERR to their predecessor nodes. This process continues until the source node is reached. When RERR is received by the source node, it can either stop sending the data or reinitiate the route discovery mechanism by sending a new RREQ message if the route is still required.

Advantages

- AODV has low control signalization because there are not periodic updates about the routing and the overload in terms of packets is small since it is a reactive protocol. Also, the processing signalization is low because the AODV messages are simple and require small calculus. Besides, the loops are solved.
- AODV is a simple protocol that aims to resolve more recent and shorter paths. DSR, on the other hand, employs multiple optimizations, which in some cases result into worse performance e.g. invalid route pollution due to aggressive route learning and caching.

Disadvantages

- AODV works only with bidirectional links. Although AODV only manages the routes between nodes who want to communicate, it uses Hellos messages periodically. Thus, in comparison with DSR overhead in terms of packets is higher.
- Inconsistent route may appear.
- Multiple RREP can lead to heavy control overhead.
- Periodic beaconing.

C. ***TORA (Temporally Ordered Routing Algorithm)***

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. 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, Route maintenance and Route erasure. During the route creation and maintenance phases the nodes use a "height" metric, which establishes a Direct Acyclic Graph (DAG) rooted at the destination. Therefore, links are assigned a direction (upstream or downstream) based on the relative height metric of neighboring nodes. The process for establishing a DAG is similar to the *Query/Reply* process in Lightweight Mobile Routing (LMR). In times of node mobility, the DAG route is broken and route maintenance is necessary to re-establish a DAG rooted at the same destination. Timing is an important factor for TORA because the *height* metric depends on the logical time

of link failure. TORA assumes all nodes to have synchronized clocks. In TORA, there is a potential for oscillations to occur, especially when multiple set of coordinating nodes are concurrently detecting partitions, erasing routing, and building new routes based on each other. Because TORA uses inter-nodal coordination, its instability problem is similar to the "count-to-infinity" problems.

Advantages

The advantage of TORA is that the multiple routes are supported by this protocol between the source and destination node. Therefore, failure or removal of any of the nodes is quickly resolved without source intervention by switching to an alternate route to improve congestion. It does not require a periodic update, consequently communication overhead and bandwidth utilization is minimized. It provides the support of link status sensing and neighbor delivery, reliable in-order control packet delivery and security authentication.

Disadvantages

Also TORA consist some of the limitations like which depends on synchronized clocks among nodes in the ad hoc network. The dependence of this protocol on intermediate lower layers for certain functionality presumes that the link status sensing, neighbor discovery, in order packet delivery and address resolution are all readily available. The solution is to run the Internet MANET Encapsulation Protocol at the layer immediately below TORA. This will make the overhead for this protocol difficult to separate from that imposed by the lower layer.

IV. Comparison Between Routing Protocols

Table 1 Comparison between AODV, DSR and TORA [6]

Comparison Parameters	AODV	DSR	TORA
Source Routing	No	Yes	No
Topology	Full	Full	Reduced
Update Information	Route Error	Route Error	Node's Height
Update routing table periodically	Yes	No	No
Method	Unicast, Broadcast	Unicast, Broadcast	Broadcast
Update Destination	Source, Neighbour	Source	Neighbour
Loop Freedom Maintenance	Sequence Number	Source route	Establish a directed acyclic graph
Multiple Path	No	Yes	Yes
Support one way link	No	Yes	No
Mechanism of routing	Next Hop	Shortest Routing	Next Hop

V. Result And Analysis Of Routing Protocols

MANET has number of qualitative and quantitative metrics that can be used to compare ad hoc routing protocols. Following metrics are considered to evaluate the performance of ad hoc network routing protocols using MATLAB as follows: [7]

A. *Throughput*

Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

Fig. 2 Throughput among AODV, DSR and TORA

B. *Load*

The load in the network specifies how the traffic is distributed among the nodes.

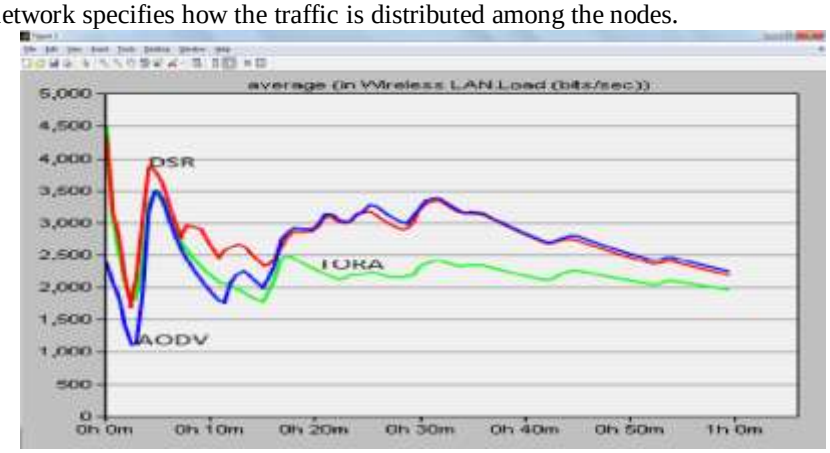

Fig. 3 Load among AODV, DSR and TORA

C. *Delay*

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds.

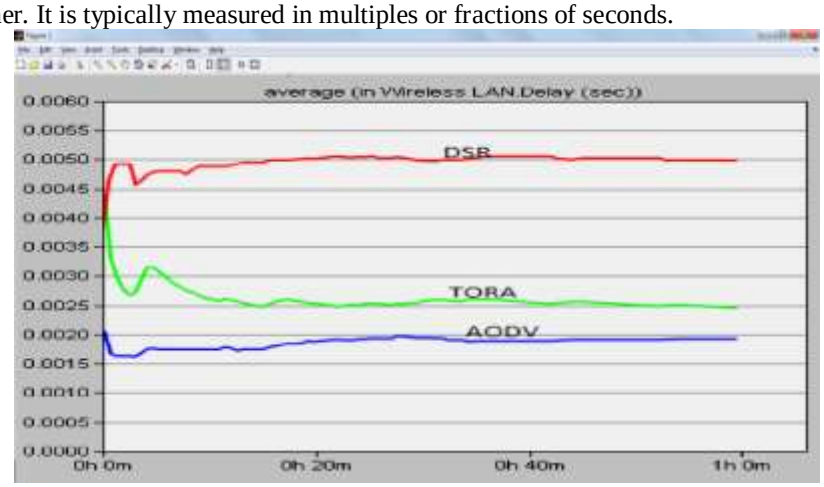

Fig. 4 Delay among AODV, DSR and TORA

VI. Future Work

Much of the effort has been conducted to support efficient communication between nodes which are parts of MANETs. It is really difficult to design a routing protocol which satisfies all the issues mentioned so far in this paper. Moreover, this field of research is a state-of-the-art and ongoing topic which many papers are still conducting to highlight and review different existing routing protocols. The importance of this type of research is proven by increasing number of survey researches which try to compare different protocols, some of these up-to-date surveys are presented in. According to this overview still there are many open research topics in MANETs that deserve more investigation. Moreover, as an interesting future work of this research, it would be valuable to evaluate the well-known routing protocols that have been suggested for MANETs based on the quantitative metrics. There should be some a standardized intrusion detection techniques can be used and the techniques which already have get further improved. The current evaluation for state-of-the-art wireless security solutions is quite ad hoc. There are some drawbacks which should be improved.

VII. Conclusion

MANETs have received increasing research attention in recent years. There are many active research projects concerned with MANETs. Mobile ad hoc networks are wireless networks that use multi-hop routing instead of static networks infrastructure to provide network connectivity. MANETs have applications in rapidly deployed and dynamic military and civilian systems. The network topology in MANETs usually changes with time. Therefore, there are new challenges for routing protocols in MANETs since traditional routing protocols may not be suitable for MANETs. This work is an attempt towards a comparative study of commonly used mobile ad hoc routing protocols (DSR and AODV). Over the past few years, new standards have been introduced to enhance the capabilities of ad hoc routing protocols. As a result, ad hoc networking has been receiving much attention from the wireless research community. We can summarize our final conclusion as:

- Increase in the density of nodes yields to an increase in the mean End-to-End delay.
- Increase in the pause time leads to a decrease in the mean End-to-End delay.
- Increase in the number of nodes will cause increase in the mean time for loop detection.

In short, 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.

References

[1] David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. Technical report, Carnegie Mellon University, 1996.
[2] Mehran Abolhasan, Tadeusz Wysocki, and rykDutkiewicz. A review of routingprotocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia,2003.
[3] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. 2002.
[4] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Technical report, Nokia Research Center; University of California, Santa Barbara; University of Cincinnati, November 2001. draft-ieftaodv-09.txt - work in progress.
[5] David B. Johnson, Yih-Chun Hu, David A. Maltz, Jorjeta G. Jetcheva. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR).
[6] Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.
[7] S R Chaudhary, A Al Khwildi, Y Casey, H Aldelou, H S Al Raweshidy. A Performance Comparison of Multi On-Demand Routing in Wireless AdHocNetworks.