IJCSC 0973-7391 Vol 6 • Number 2 April - Sep 2015 pp. 368-371 **Impact Factor: 2.5** **Available at** www.csjournals.com

Routing Protocols in MANETS: A Review

Suraj Pal
Assistant professor, Deptt. of computer science, University College, KUK, India
suraj.nehra1@gmail.com

Abstract: The dynamic nature of the networks demands new set of networking strategies to be implemented in order to offer efficient end-to-end communication. These, along with the various application of these networks in various scenarios such as disaster recovery and battlefield, have seen MANETs being researched by many different organizations. MANETs utilize the traditional TCP/IP structure to offer end-to-end communication between nodes. However, due to their mobility and the use of limited resource in wireless networks, each layer in the TCP/IP model requires modifications to function in MANETs. One attractive research area in MANET is routing also it is very challenging task and has received a great amount of attention. This has led to development of various routing protocols for MANETs, and each author of each proposed protocol argue that the approach proposed provides an enhancement over a number of various approach or strategies considered in the literature for a specified network scenario. Therefore, it is fairly difficult to determine which protocols may achieve best under a number of different network conditions, such as increasing node density and traffic. In this paper, we discussed an overview of a wide range of routing protocols proposed in the past.
Keywords: Security attacks, routing protocol, ad-hoc review

1. INTRODUCTION

The most recent advancement in wireless technology and its applications received a great amount of attention. An ad hoc network is one such modern technology, which gives a new standard for wireless self-organized networks. Ad hoc networks are simple peer-to peer, self- organized networks and with no fixed infrastructure. Ad-hoc network is a model in computer communication which means that user wanting to communicate with each other forms a temporary network connection, without use of central administration. Each node in the ad hoc network acts both as host and router, and must therefore ready to forward packet for other node. A Mobile Ad-hoc Network (MANET) is a temporary wireless network made up of mobile nodes without any stable infrastructure. Each node acts as a router to forward packets on behalf of other nodes. One of the preeminent features of MANET is its flexibility and can organize itself in the fly and thus very appropriate for the emergency situation.

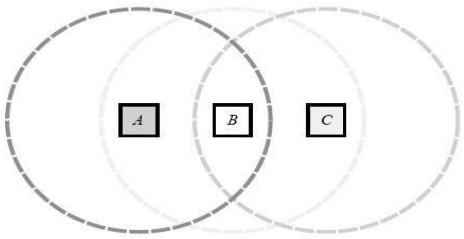

Fig.1 A Simple MANET

In figure 1, let's assume that node A try to send data to node C but node C is not in the range of node A. Then in this case, node A may use the services of node B to transmit data since node B's range overlaps with both the node A and node C. Certainly, the routing problem in a real ad hoc network may be more complex than this example suggests, due to the intrinsic non uniform propagation distinctiveness of wireless transmissions and due to the possibility that any of the hosts concerned may move at any time. One of the major difficulties in MANET (Mobile Ad hoc Network) is the packet routing problem, which is provoked by frequent topology changes due to movement of nodes, network partitions and radio interference. Many Routing protocols have been planned in past and reported in the literature. The proactive approaches tries to maintain routing information for all nodes in the network at all times, where as the reactive approaches only find out new routes when necessary and other approaches make use of geographical position information for routing.

2. SECURITY ATTACKS

Mobile ad hoc networks can have various types of attacks. In Mobile ad hoc network, attacks can be categorized into Passive Attacks and Active Attacks. Brief introduction of these attacks are as follow:

A. Passive Attacks- In these attacks, attackers don't interrupt the operation of routing protocol but only try to discover valuable information by listening to the routing traffic. The attacker only looks the transmission and does not try to change the data packets. Two types of passive attacks are as follows:-

Traffic analysis: In traffic analysis attack, attacker observes packet transmission to gather important information such as a source, destination and source-destination pair information.

Eavesdropping: In Eavesdropping attack, attackers acquire some confidential information e.g. location, private key, public key, even password of the node that should be reserved secret during transmission.

B. Active Attacks- In these attacks, the malicious nodes establish false information to puzzle the network topology. They can either attract traffic to them or then drop the packets. They can also send false information and transfer packets to the wrong node and cause congestion in that area. Different types of active attacks are:

Sinkhole Attack: A sinkhole node tries to magnetize or attract the data toward itself from each and every neighboring node. In this attack, a malicious node produces fake routing information and show itself as authorized nodes for the route.

Flooding Attack: In this attack, a malicious node may also insert false packets to consume the accessible resources onto the network, so that legitimate user can not able to use the network resources for legal communication.

Replay: This attack generally targets the freshness of routes. In replay attack an attacker record the message and then retransmit the old message to the other nodes to make update their routing table to old routes.

Rushing Attack: In Rushing attack, attacker forwards routing packets as speedy as possible to gain access to multicast forwarding group before the valid node .By this way rushing attack can deliberate down the performance of network.

C. Common attacks in MANETs:-

1. Denial-of-service:-In the denial-of-service attack, a malicious node can successfully transmit an erroneous route message to the source node to disrupt the service.

2. Tunnelling Attack: - Tunnelling attack is that where two or more nodes may work together to encapsulate and exchange messages between them along accessible data routes.

3. Wormhole Attack: - In Wormhole an attacker reports packet at one location, tunnels them to another location, and retransmits them back into the network. This wormhole attack is possible even if the attacker has not cooperate with any hosts and even if all communication ink provides authenticity and confidentiality in the network.

4. Black hole Attack:-In Black hole attack a malicious node utilizes the routing protocol to publicize itself as having the shortest path to the node whose packets it wants to interrupt and in this way it can compromise the service.

3. ROUTING PROTOCOLS

There are various secure routing protocols proposed which are based on the working principles of the earlier ad hoc routing protocols.

SEAD: (Secure efficient ad hoc distance vector routing protocol).SEAD is based on the DSDV (Destination Sequenced Distance Vector) protocol. SEAD was developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig.

DSDV: Destination Sequenced Distance Vector routing protocol is the earliest protocol proposed for ad hoc wireless networks. It was based on the distributed Bellman Ford algorithm where each and every node maintains a table that includes the shortest distance and the very first node on the shortest path to every other node in the network. DSDV is a table driven routing protocol. Routes to all destination nodes are readily available at every node at all times. The tables are exchanged between neighbours at usual intervals to keep an updated view of the network topology. Whenever there is a modification in the network topology, the table entries are updated. It

offer loop free single path to the destination. DSDV transmit two types of packets "full dump" and "incremental".

Ariadne: Ariadne is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig, based on the Dynamic Source Routing protocol (DSR). It is relied on unidirectional link support.

DSR: DSR is an on-demand routing protocol, which find out the route as and when required, dynamically. DSR routing protocol maintain the network without any centralized administrator or infrastructure. In route discovery this protocol discovers the routes from source to destination. In DSR, data packets preserved the routing information of all intermediate or middle nodes in its header to reach at a particular destination. Routing information for every source can be change at any time in the network and DSR updates this information after each change occur [7]. Intermediate routers don´t need to have routing information to route the traffic, but they save routing information for their future use. Basic purpose to develop DSR was to decrease the overhead on the network and designing self--configuring and self-organizing protocol to support MANET.

Secure Routing Protocol (SRP):

Secure Routing Protocol (SRP), was proposed by Papadimitratos and Hass [8]. SRP is implemented over DSR [4], [5], with an underlying Security Association (SA) between the source and destination nodes. The trust relation is maintained with a public key infrastructure and a shared key K(sd), was maintained between the source and destination nodes using the security association. In SRP the route request (RREQ) contains six fields and a MAC value to initiate the discovery process. The RREQ is signed with the shared key K(sd) between the source and destination. The intermediate nodes participating in the route discovery measures the frequency of queries received from their neighbours and maintains a priority ranking inversely proportional to the query rate. So if a malicious node participates in the network with malicious RREQ's will be dealt last in the priority list.

ARAN: Authenticated routing for Ad hoc Network

KimayaSanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz and Elizabeth M.Belding-Royer proposed Authenticated routing for Ad hoc Network based on AODV.

AODV (Ad hoc On Demand Distance Vector) routing protocol uses an on-demand approach or strategy for route discovery. It uses the idea of sequence numbers in DSDV to avoid routing loops in the network. AODV makes routes using a route request and route reply cycle. When a source node wants a route to a destination for which it does not previously have a route, it transmits a route request (RREQ) packet across the network. RREQ carries Source ID, Destination ID, Source Sequence Number, Destination Sequence Number and a Broadcast ID. When an intermediate or middle node receives a RREQ, it sends a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that enclosed in the RREQ. The intermediate or middle node also stores the previous node information in order to forward the data packet to this next node towards the destination.

SAODV: Secure Ad hoc On-Demand Distance Vector Routing

SAODV is a secure routing protocol that based on AODV. SAODV was proposed by "Manel Guerrero Zapata, N. Asokan.

SAODV in its implementation suppose that there is already a central key management system through which every node can get public keys. Digital signatures are used to validate the fields of the message and hash chains to secure the hop count information. SAODV uses hash chains to validate RREQ and RREP flows between all neighbour nodes in the route discovery process. A hash chain is formed with a one-way hash function and arbitrary seed. Every time a node created a RREQ or a RREP message, the maximum hop count field is set to the max time to live. The hash value is calculated using the hash function 'h´ and the arbitrary seed to it. Every time RREQ or RREP are received by a node it validate the hop count, [h (max hop) – hop count time] to check it with the value enclosed in the top hash value. When a node first receives a RREQ, it first validates the signature before creating or updating a reverse route to that host. When the RREQ reaches the destination node, RREP will be transmit with a RREP signature extension.

SAR: Security- Aware Routing Protocol

Seung Yi, Prasad Naldurg and Robin Kravets proposed SAR. AODV is discussed in the previous section.

So directly look into the secure mechanism included by SAR over AODV. SAR uses security as one of the major key metrics in its route discovery. The attributes and framework of the security metrics are detailed in [14]. This framework also uses various levels of security for various levels of applications.
Each node in the network is connected with a level of trust metric, based on which network route will be followed according the security requirements of the application.

SAR Features:-

- It is generally implemented over AODV.
- SAR uses security as one of the major key metrics in its route discovery.
- Hierarchical level of security can be maintained.

4. CONCLUSION

Securing ad hoc environments is a very challenging task. The main principle of this paper was to acquire knowledge of ad hoc routing protocols and secures routing protocols. Security estimation of some of the secure routing protocols are done using case study with the most usually identified attack patterns in ad hoc networks. Performance estimation of ad hoc secure routing protocols SEAD and Ariadne was done with most generally identified performance metrics.
In the secure routing protocols some of the security attacks are possible with a compromised node. From the case study results, it concludes that on demand driven protocols are less prone to security attacks than table driven protocols. Protocols based on DSR and AODV are stable to security attacks due to the strong cryptographic performance.

REFERENCES

[1] Xiang Chen, HongqiangZhai, Jianfeng Wang, and Yuguang Fang," TCP performance over mobile ad hoc networks", CAN. J. ELECT. COMPUT. ENG., VOL. 29, NO. 1/2, JANUARY/APRIL 2004.
[2] StylianosPapanastasiou, Mohamed Ould-Khaoua, Lewis M. Mackenzie," On the evaluation of TCP in MANETs", Department of Computing Science University of Glasgow Glasgow, UK G128QQ.
[3] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02) Panagiotis
[4] Basagni, S. Conti, M. Giordano, S. Stojmenovi&cacute (Edit). [2004]. Mobile Ad Hoc Networking: September 2004 Wiley-IEEE Press. (pp. 1-33, 275-300, 330-354)
[5] C. Siva Ram Murthy and B.S. Manoj. [2004]. Ad Hoc Wireless Networks, Architecture and Protocols: 2004 Pearson Education (pp. 321-386, 473-526)
[6] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.
[7] David B. Johnson, David A. Maltz, and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop WirelessAd Hoc Networks", in Ad Hoc Networking, Editor: Charles E.Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.
[8] PanagiotisPapadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.
[9] KimayaSanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer [2002]. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02).