IJITKMSpecial Issue (ICFTEM-2014) May 2014 pp. 57-60 (ISSN 0973-4414)

A Review of Routing Protocols in MANETS-Security Analysis

PrincyTyagi
M.Tech Department of Computer Science & Engineering M.V.V.E.College of Engg, Jagadhari
(Yamuana Nagar) (Haryana)
Deepak88garima@gmail.com

Abstract— The infrastructure less and the dynamic nature of these networks demands new set of networking strategies to be implemented in order to provide efficient end-to-end communication. These, along with the diverse application of these networks in many different scenarios such as battlefield and disaster recovery, have seen MANETs being researched by many different organizations and institutes. MANETs employ the traditional TCP/IP structure to provide end-to-end communication between nodes. However, due to their mobility and the limited resource in wireless networks, each layer in the TCP/IP model requires redefinition or modifications to function efficiently in MANETs. One interesting research area in MANET is routing also it is a challenging task and has received a tremendous amount of attention from re-searches. This has led to development of many different routing protocols for MANETs, and each author of each proposed protocol argues that the strategy proposed provides an improvement over a number of different strategies considered in the literature for a given network scenario. Therefore, it is quite difficult to determine which protocols may perform best under a number of different network scenarios, such as increasing node density and traffic. In this paper, we provide an overview of a wide range of routing protocols proposed in the literature.
Keywords:- Security attacks, routing protocol, ad-hoc review

1. INTRODUCTION

The latest advancement in wireless technology and its applications received a lot of attention. An ad hoc network is one such recent technology, which gives a new paradigm for wireless self-organized networks. Ad hoc networks are simple peer-to peer networks, self- organized and with no fixed infrastructure. Ad-hoc network is a concept in computer communication which means that user wanting to communicate with each other forms a temporary network, without use of centralized administration. Each node in the network acts both as host and router and must therefore willing to forward packet for other node. A Mobile Ad-hoc Network (MANET) is a temporary wireless network composed of mobile nodes without any permanent infrastructure. Each node not only operates as an end system, it also acts as a router to forward packets on behalf of other nodes. One of the best features of MANET is its flexibility and can configure itself in the fly and thus very suitable for the emergency situation.

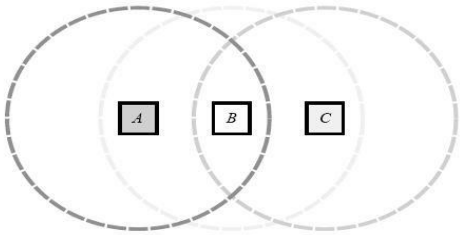

Fig.1 A Simple MANET

In figure 1, let's suppose that node A wants 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 transfer data since node B's range overlaps with both the node A and node B. Indeed, the routing problem in a real ad hoc network may be more complicated than this example suggests, due to the inherent non uniform propagation characteristics of wireless transmissions and due to the possibility that any or all of the hosts involved may move at any time. One of the main difficulties in MANET (Mobile Ad hoc Network) is the routing problem, which is aggravated by frequent topology changes due to node movement, radio interference and network partitions. Many Routing protocols have been proposed in past and reported in the literature. The proactive approaches attempts to maintain routing information for each node in the network at all times, where as the reactive approaches only find new routes when required and other approaches make use of geographical location information for routing

2. SECURITY ATTACKS

Mobile ad hoc network can be subject to many types of attacks. In Mobile ad hoc network, attacks can be classified into Passive Attacks and Active Attacks. Brief introduction of both attacks are as follow:

A. Passive Attacks- In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. The attacker only looks and watches the transmission and does not try to modify or change the data packets. Two types of passive attacks are;-

Traffic analysis: In this attack, attacker monitors packet transmission to infer important information such as a source, destination and source-destination pair.

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

B. Active Attacks- In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area.Various types of active attacks are:

Sinkhole AttackA sinkhole node tries to attract the data toward itself from all neighboring nodes. In this attack, a malicious node generates fake routing information and show itself as legal nodes for the route.

Flooding Attack In this attack, a malicious node may also inject false packets to consume the available resources onto the network, so that valid user can not able to use the network resources for valid communication.

ReplayThis attack usually targets the freshness of routes. In this attack an attacker firstly record the message and then resend the old message to the other nodes to make update their routing table to stale routes.

Rushing Attack In Rushing attack, attacker forward routing packets as quick as possible to gain access to multicast forwarding group before the legal node .By this way rushing attack can slow down the performance of network.

C. Common attacks in MANETs:-

1. Denial-of-service with modified source route:-In the denial-of-service, a malicious node in between can successfully send an erroneous route message to the source route to disrupt the service.

2. Tunnelling Attack:-In tunnelling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes.

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

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

3. Routing Protocols

There are several secure routing protocols proposed basing on the working principles of the earlier ad hoc protocols.

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

DSDV: Destination Sequenced Distance Vector routing protocol is one of the first protocol proposed for ad hoc wireless networks. It was developed based on the distributed Bellman Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. It's a table driven routing protocol. Routes to all destinations are readily available at every node at all times. The tables are exchanged between neighbours at regular intervals to keep an up-to-date view of the network topology. Whenever there is a change in the network topology, the table entries are updated. It provides loop free single path to the destination. DSDV sends 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 based on unidirectional link support.

DSR: DSR is an on-demand routing protocol, which finds the route as and when required, dynamically. DSR routing protocol manage the network without any centralized administrator or infrastructure. In route discovery this protocol discovers for the routes from source node to destination. In DSR, data packets stored the routing information of all intermediate nodes in its header to reach at a particular destination. Routing information for every source node can be change at any time in the network and DSR updates it after each change occur [7]. Intermediate routers don´t need to have routing information to route the passing traffic, but they save routing information for their

future use. Basic purpose to develop DSR was to reduce the overhead on the network and designing self-organizing and self-configuring 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 developed Authenticated routing for Ad hoc Network based on AODV.
AODV (Ad hoc On Demand Distance Vector) routing protocol uses an on-demand approach for route discovery. It uses the concept of sequence numbers in DSDV to avoid routing loops. AODV builds routes using a route request and route reply cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts 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 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 contained in the RREQ. The intermediate 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 developed based on AODV. SAODV was developed by "Manel Guerrero Zapata, N. Asokan.
SAODV in its implementation assume that there is already a central key management system through which every node can obtain public keys. Digital signatures are used to authenticate the fields of the message and hash chains to secure the hop count information. SAODV uses hash chains to authenticate RREQ and RREP flows between neighbour nodes in the route discovery process. A hash chain is formed with a one-way hash function and random seed. Every time a node originates a RREQ or a RREP message, the maximum hop count field is set to the max time to live. The top hash value is calculated using the hash function 'h′ and the random seed to it. Every time RREQ or RREP are received by a node it verifies the hop count, [h (max hop) – hop count time] to check it with the value contained in the top hash value. When a node first receives a RREQ, it first verifies the signature before creating or updating a reverse route to that host. When the RREQ reaches the destination node, RREP will be sent with a RREP signature extension.

SAR: Security- Aware Routing Protocol
Seung Yi, Prasad Naldurg and Robin Kravets developed SAR. AODV is discussed in the previous section.
So directly look into the secure mechanism incorporated by SAR over AODV. SAR uses Security as on of the Key Metrics in its route discovery and maintenance. The framework and attributes of the security metrics are detailed in [14]. This framework also uses different levels of security for different level of applications.
Each node in the network is associated with a level of trust metric, based on which route will be followed according the security requirements of the application

SAR Features:-
- It is mainly implemented over AODV.
- SAR uses Security as on of the Key Metrics in its route discovery and maintenance.
- Hierarchical level of security can be maintained.

4. Conclusion

Securing ad hoc environments is a challenging task. The main purpose of this thesis work was to acquire in-depth knowledge of ad hoc routing protocols and secures routing protocols. Security evaluation of some of the secure routing protocols are done using case study with the most commonly identified attack patterns in ad hoc networks. Performance evaluation of ad hoc secure routing protocols SEAD and Ariadne was done with most commonly identified performance metrics.

In the secure routing protocols most of the security attacks are possible with a compromised node. From the case study results, it concludes that table driven protocols are more prone to security attacks than on demand driven protocols. Protocols based on DSR and AODV are more stable to security attacks due to the strong cryptographic implementation.

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).