Vulnerabilities for Reactive Routing in Mobile Adhoc Networks

Parveen Kakkar[1] Krishan Kumar Saluja[2]
1.Department of Computer Science and Engineering, DAVIET, Jalandhar, India
2.Department of Computer Science and Engineering, SBSSTC, Ferozepur, Punjab, India
*Corresponding Author: Email: parveen.daviet@gmail.com, k.salujasbs@gmail.com

Abstract
Mobile ad hoc network got outstanding success as well as tremendous attention due to its self -maintenance and self-configuration properties or behavior. This paper presents the area of wireless network i.e. work on ad-hoc network. This paper presents protocols of routing and their classification and their comparison. This paper also presents security issues of wireless network. This paper provides an overview of the security issues in MANETs. It classifies the attacks that are possible against the existing routing protocols. An understanding of these attacks and their impacts on the routing mechanism will help researchers in designing secure routing protocols.

Keywords: MANET, AODV, DSR, FLOODING.

1. Introduction to MANET

Mobile Ad hoc Network is a system of mobile nodes which are self organizing without the central control system. As the topology is not fixed it can be operated in any environment. Addition and deletion of nodes is easy. Although it provides more flexibility, but it brings more challenges to routing in MANET also battery consumption should be less.

Fig. 1. Mobile Ad hoc Network [10]

In MANET, a wireless node can be the source of data transmission, destination or intermediate node. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. A node playing the role of a router may get out of the route between source and destination then the route is disconnected, and route discovery process has to be restarted. Thus, the main goal of routing protocol in MANET is to find a correct route efficiently. Some typical examples include emergency search-rescue operations, meeting events, conference, and battlefield communication between moving vehicles or soldiers.

1.1. Routing in MANET

Routing in MANETs is a dynamic optimization task aiming at providing paths that are:

- Optimum in terms of some criterion (e.g. minimum distance, maximum bandwidth, shortest delay).
- Satisfying some constraints (e.g. limited power of mobile nodes, limited capacity of wireless links).

1.2. Protocols Classification

Routing protocols are mainly classified into three types:-

1. Proactive Routing Protocols
2. Reactive Routing Protocols
3. Hybrid Routing Protocols

1.2.1 Proactive Routing Protocols

In proactive approach nodes will maintain the tables in which information about other nodes are kept in advance. Information is exchanged with other nodes periodically; any change in topology will be updated in all the tables. Mainly used proactive protocols are OLSR, DSDV and OSPF etc.[4][5][9]

1.2.2 Reactive Routing Protocols

Reactive protocols used on demand approach i.e. whenever any node wants to communicate to some other node only then the link between two will be established. Because reactive protocols save bandwidth by exchanging the information when required, so these are mainly used and more popular. Mainly used reactive protocols are

AODV, DSR and DYMO etc.[2][3]

Fig. 2. Classification of Routing Protocols [1]

1.2.2.1 Dynamic Source Routing (DSR) Protocol

The Dynamic Source Routing Protocol [7] is an on-demand routing protocol which is based on the concept of source routing. Dynamic Source Routing (DSR) composed of two parts: Route Discovery and Route Maintenance [6]. In this two commands are used i.e. ROUTE REQUEST and REPLY.

1.2.2.2 Ad hoc On-demand Distance Vector (AODV) Routing Protocol

The Ad hoc On-demand Distance Vector routing protocol [8] inherits the good features of both DSDV and DSR. Ad hoc On-demand Distance Vector Routing (AODV) [2] protocol is an on demand routing protocol [8] as it determines a route to the destination only when a node wants to send data to that destination. The source broadcasts a route request (RREQ) packet when it wants to find path to the destination.

Route Discovery

During the route discovery process, the source node broadcasts RREQ packets similar to DSR. The RREQ packet contains the source identifier (SId), the destination identifier (DId), the source sequence number (SSeq), the destination sequence numbers (DSeq), the broadcast identifier (BId) and TTL fields. When an intermediate node receives a RREQ packet, it either forwards it or prepares a Route Reply (RREP) packet if it has a valid route to the destination in its cache.

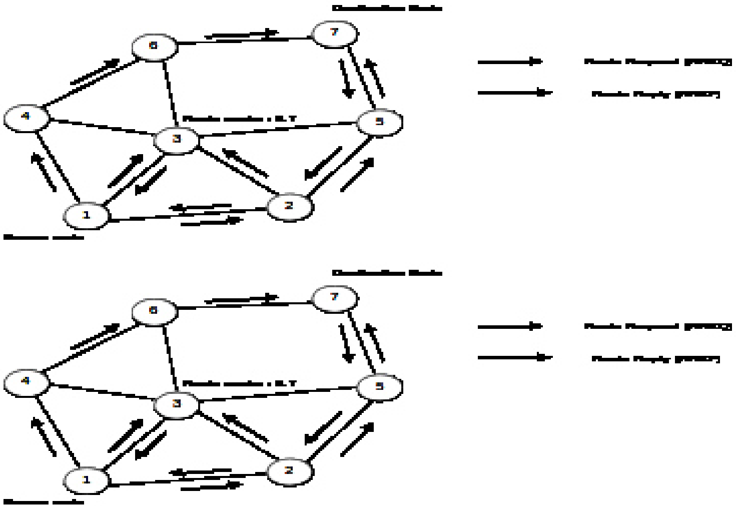

Fig. 3. Route discovery in AODV [8]

Route Maintenance

The route maintenance mechanism works as follows – Whenever a node detects a link break by link layer acknowledgements or HELLO beacons [2], the source and end nodes are notified by propagating an RERR packet similar to DSR.

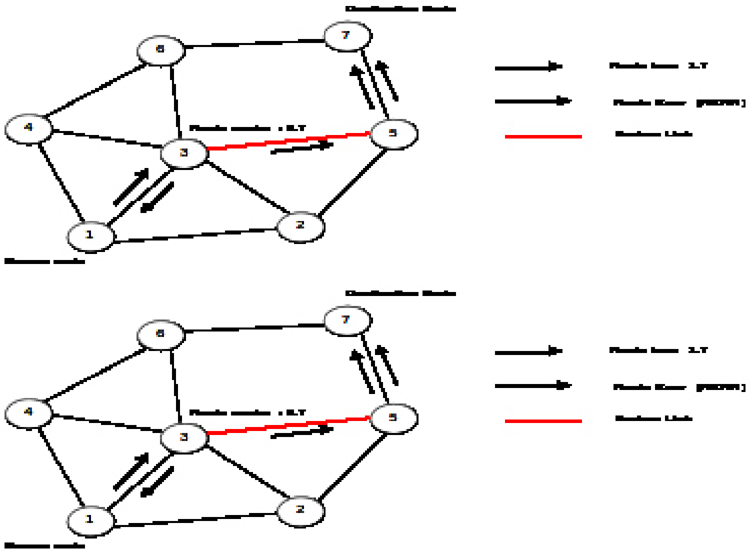

Fig. 4. Route Maintenance in AODV [8]

1.2.2.3 Comparison of DSR and AODV

Protocol **Feature**	**DSR**	**AODV**
Destination sequence numbers	Not used	Used
Link Layer acknowledgements	Not Required	Required (using HELLO beacons) for link breakage detection
Routing mechanism	Source routing – Multiple route caches for each destination	Table driven – one entry per destination. Sequence numbers used for
Route storage mechanism	Using route caches	Using routing tables
Timers	Not Used	Used
Multiple Route caches	Yes	No
Optimizations	Salvaging, Gratuitous route replies (RREP) and Route Error (RERR), non-propagating route requests [11]	Expanding ring search [10]

Table 1: Comparison of the features of DSR and AODV

1.2.2.4 Pros and Cons of Reactive Routing Protocols

- The main advantage of proactive routing protocols is that periodic routing updates are not required. Thus, the number of routing packets in the network is reduced thereby decreasing the load on the network.
- Link breakages are detected by a route maintenance mechanism only when needed in contrast to table driven protocols which maintain updated routes by propagating periodic updates.
- In general, on demand routing protocols have found to perform better under higher mobility rates of nodes and exhibit low latency in moderate to large networks [10].

1.3 Hybrid Routing Protocols

Hybrid routing protocols inherit the characteristics of both on-demand and table-driven routing protocols. Such protocols are designed to minimize the control overhead of both proactive and reactive routing protocols.

2 Security Issues

Due to different characteristics of Mobile ad hoc network security is an active research topic in wireless path, which is also a nontrivial challenging to security design.[4][6][10] There are different types of challenges in mobile ad hoc network which are given below:

- Open network architecture
- Shared wireless medium
- Stringent resource constraints
- Highly dynamic network topology

3 Categorization of attacks in MANET

Attacks can be categorized into two types on the basis of behavior

1) Passive Attacks
2) Active Attacks

3.1 Passive attacks:

This kind of attack targets at collecting valuable information from the network. The information includes transferred data, the identification of communicating nodes, node location and network topology. Eavesdropping is the most simple and effective type of wireless attack. This kind of attach leaves no trace of the hacker's presence on or near the network. This kind of attack is also the most difficult to be detected. [5][8]

3.2. Active Attacks

3.2.1. Jamming

Jamming is a technique that would be used to simply corrupt the network. Similar to denial of service attacks on internet application servers such as HTTP and FTP. MANET can be corrupted by overwhelming radio frequency (RF) signal[6].

3.2.2. Denial of Service - DoS

Distributed DoS attack is a more severe threat: if the attackers have enough computing power and bandwidth, smaller MANETs can be crashed or congested very easily. Radio jamming and battery exhaustion are two ways in which nodes cannot communicate with each other.

3.2.3 Impersonation

If authentication of nodes is not supported, malicious nodes can be able to join the network without detection, send false routing in formation, and masquerade as some other trusted node.

3.2.4 Fabrication

There are three kinds of fabrication attacks.

- To generate route error messages.
- To corrupt routing information.
- Other fabrication attacks

The first one is to generate false routing packet. The second one is to corrupt routing information. The third one is to produce a lot of false routing information and to flood the network. In any case, these kinks of attacks are not easy to detect.

4 Flooding Attack in MANET

It is of two types

4.1. Data Flooding: - In data flooding attacker will send unwanted data items to congest the network. Once the paths are established between all the nodes attacker will flood unwanted data packets, which will ultimately causes to Denial of Service.[11]

4.2. RREQ Flooding: - Attacker will send large amount of RREQ requests to waste the bandwidth and resources of the network, usually the destination IP chosen for RREQ will not exists in the network , so no node knows the location of the required IP , as a result the RREQ will pass through whole the network. Any destination node will always be busy in receipt of unwanted data. [11][12]

Fig. 5. RREQ Flooding Attack in MANET [11]

5 Summary

There have been several routing protocols proposed for MANETs. Although MANETs provide unique advantages, they are faced with unique challenges as well, such as the dynamic topology, bandwidth constraint, media interference, etc. Among them, the security of the routing protocols always plays a vital role in MANET. This paper provides an overview of the security issues in MANETs. It classifies the attacks that are possible against the existing routing protocols. An understanding of these attacks and their impacts on the routing mechanism will help researchers in designing secure routing protocols.

5.1 Brief Literature Survey

Sr. no	Title	Aim	Good points	Bad points	Simulator used	Possible contribution
1	Securing Ad hoc Routing Protocols	Applied cryptographic techniques to authenticating routing traffic and can prevent external intruders or malicious insiders .	1)Provide Authentication 2)Can Avoid Data Flooding Attacks	Cannot prevent from RREQ Flooding Attack	NA	Some Filtering mechanism can be used to filter the RREQ messages
2	Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc net.	To avoid the RREQ flooding attack, Route discovery chains are used to rate-limit the number of route discoveries.	1) This limits the impact of RREQ flooding attack on the network. 2) Effective Bandwidth Utilization	If the no. of forged RREQs generated is large, genuine RREQ attempts never sent.	NS-2	While assigning the chains to the nodes, reputation of the nodes must be the criteria.
3	Mitigating Malicious Control Packet Floods in Ad Hoc Networks	To defend against malicious control packet floods like RREQ flooding attack, Adaptive statistical packet dropping mechanism is proposed	1) Efficient Bandwidth Utilization 2) Throughput is high.	Dropping RREQ will lead to the reduction of throughput of the network.	Glomosim	Threshold should be dynamic on the basis of network conditions
4	Resisting Flooding Attacks in Ad Hoc Networks	To defend from RREQ Flooding ,priority system is used to determine the transmission priority of RREQs	When the malicious node broadcast excessive RREQs, the priorities of its RREQs are reduced	Cannot distinguish between genuine and forged RREQs	NS2	Bursty traffic& attack traffic should differentiated, before dropping
5	Mitigating Route Request Flooding Attacks in Mobile Ad Hoc net..	To mitigate the effect of denial of service attacks by flooding with RREQs to unreachable destinations	1)Throughput is high 2) Efficient Bandwidth Utilization	The main shortcoming is that it can't isolate malicious nodes	NS2	Mechanism should be implemented to distinguish between attack traffic and bursty traffic.
6	Framework for statistical filtering against DDoS attacks in MANETs	To defend from flooding Attack proposed a framework for statistical filtering in MANETs which make use of a cluster-based approach.	1)Cross-layer mechanism is implemented in filters. 2)provides better detection of attack.	Routing overload is more.	Glomosim	Shared Information between layers should be less.
7.	Infrastr. and algo's for distributed anomaly-based intrusion detection in mobile ad-hoc net.	To detect the attack, collecting raw data of network operation, is collected and computing a local anomaly index measuring the difference between the current node operation and a baseline of normal operation.	1)Clustering is applied at three levels, provides better detection. 2) Load is equally distributed among nodes	1)False detection rate is high. 2)Difficult to identify normal operation.	NS2	Normal operation should be decided carefully to reduce false alarm rate.
8	Mitigating Flooding Attacks in Mobile Ad-hoc Networks	To propose a novel technique in which to identify and isolate the malicious nodes which flood the whole network	1) Nodes are given chance to again joins the network. 2) False Alarm rate is very less	Routing overhead increased	NS2	The nodes will choose the better threshold tuple.

References

[1] Jhaveri, R.H. Patel, S.J. Jinwala and D.C. , "DoS Attacks in Mobile Ad Hoc Networks: A Survey," *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* , vol., no., pp.535-541, 7-8 Jan. 2012

[2] Djahel, S. Nait-abdesselam, and F. Zonghua Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges," *Communications Surveys & Tutorials, IEEE* , vol.13, no.4, pp.658-672, Fourth Quarter 2011

[3] Konate, K. Abdourahime and G , "Attacks Analysis in Mobile Ad Hoc Networks: Modeling and Simulation," *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on* , vol., no., pp.367-372, 25-27 Jan. 2011

[4] Bandyopadhyay, A. Vuppala, S. Choudhury and P. , "A simulation analysis of flooding attack in MANET using NS-3," *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), 2011 2nd International Conference on* , vol., no., pp.1-5, Feb. 28 2011-March 3 2011

[5] C. Perkins and P Bhagwat, “Highly Dynamic Destination Sequenced Distance Vector Routing DSDV for mobile computers”. In ACM SIGCOMM’94 Conference on Communication Architectures, protocols and applications, 1994, pp. 234-244.
[6] C.E. Perkins, E. Belding Royer, and S.R. Das, “Ad hoc On demand distance vector (AODV) routing”, IETF RFC 3561, July 2003.
[7] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.
[8] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, Springer, 2009
[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.
[10] Kannhavong, B. Nakayama, H. Nemoto, Y. Kato, N. Jamalipour, and A. , "A survey of routing attacks in mobile ad hoc networks," *Wireless Communications, IEEE* , vol.14, no.5, pp.85-91, October 2007
[11] M. G. Zapata and N. Asokan, “Securing Ad hoc Routing Protocols”, *Proceedings of the AC Workshop on Wireless Security (WiSe 2002),* September 2002, pp. 1-10
[12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks”, *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, ACM, Atlanta, GA, September 2002, pp. 12-23
[13] Zapata, Manel Guerrero, and Nadarajah Asokan. "Securing ad hoc routing protocols." Proceedings of the 1st ACM workshop on Wireless security. ACM, 2002.
[14] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." Wireless networks 11.1-2 (2005): 21-38.
[15] Desilva, Saman, and Rajendra V. Boppana. "Mitigating malicious control packet floods in ad hoc networks." Wireless Communications and Networking Conference, 2005 IEEE. Vol. 4. IEEE, 2005.