ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I4M6-072012

VOLUME 2 ISSUE 4 July 2012

VARIOUS ROUTING ATTACKS IN MOBILE AD-HOC NETWORKS

Ankita Gupta
Jayoti Vidyapeeth Women's University
Jaipur(Rajasthan). INDIA

Sanjay Prakash Ranga
HOD Computer Science Deptt,
Govt. Engineering College of Bikaner,
Bikaner(Rajasthan). INDIA

Abstract

A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. For this various routing protocols are used in mobile ad hoc networks as AODV, OLSR, DSDV, etc. The security of these protocols is compromised by the various types of attacks. In this paper we discuss that how these attacks affect the routing protocols in MANET.

Keywords:- MANET, Ad hoc Networks, routing , attacks.

1. INTRODUCTION

MANETs are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure (base station) for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. Routing in mobile ad- hoc networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility. A number of protocols have been developed to accomplish this task.

On a wired network, an intruder would need to break into a machine of the network or to

physically wiretap a cable. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer (and possibly a directional antenna). Hence, by simply being within radio range, the intruder has access to the network and can easily intercept transmitted data without the sender even knowing (for instance, imagine a laptop computer in a vehicle parked on the street eavesdropping on the communications inside a nearby building). As the intruder is potentially invisible, it can also record, alter, and then retransmit packets as they are emitted by the sender, even pretending that packets come from a legitimate party.

Furthermore, due to the limitations of the medium, communications can easily be perturbed; the intruder can perform this attack by keeping the medium busy sending its own messages, or just by jamming communications with noise.

MANETs provide a possibility of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with fixed infrastructure, mobile nodes in ad hoc networks do not communicate via access points (fixed structures). Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network.

Today there are various routing protocols for MANETs such as Destination- Sequenced Distance Vector routing (DSDV) [9], Dynamic Source Routing (DSR) [8], and AODV [2]. DSDV is a table driven routing protocol. In DSDV, each mobile node in the network maintains a routing table with entries for every possible destination node, and the number of hops to reach them. The routing table is periodically updated for every change in the network to maintain consistency. This involves frequent route update broadcasts. DSDV is inefficient because as the network grows the overhead grows as O(n2) [1]. DSR is an on-demand routing protocol and it maintains a route cache, which leads to memory overhead. DSR has a higher overhead as each packet carries the complete route, and does not support multicast. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors.

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V2I4M6-072012

VOLUME 2 ISSUE 4 July 2012

2. ISSUES RELATED TO ROUTING IN MOBILEAD-HOC NETWORKS

2.1 Infrastructure. An Ad-hoc network is an infrastructure less network. Unlike traditional networks there is no pre-deployed infrastructure such as centrally administered routers or strict policy for supporting end-to-end routing. The nodes themselves are responsible for routing packets. Each node relies on the other nodes to route packets for them. Mobile nodes in direct radio range of one another can communicate directly, but nodes that are too far apart to communicate directly must depend on the intermediate nodes to route messages for them.

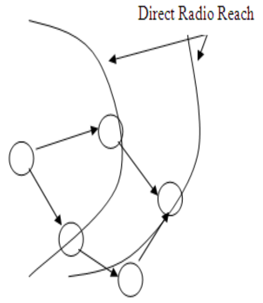

Fig 2(a) Routing in Ad-hoc networks

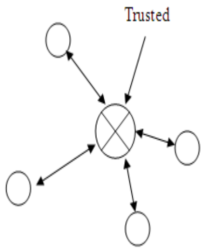

Fig 2(b) Routing in traditional networks using

2.2 Frequent changes in network topology. Ad-hoc networks contain nodes that may frequently change their locations. Hence the topology in these networks is highly dynamic. This results in frequently changing neighbors on whom a node relies for routing. As a result traditional routing protocols can no longer be used in such an environment. This mandates new routing protocols that can handle the dynamic topology by facilitating fresh route discoveries.

2.3 Problems associated with wireless communication. As the communication is through wireless medium, it is possible for any intruder to tap the communication easily. Wireless channels offer poor protection and routing related control messages can be tampered. The wireless medium is susceptible to signal interference, jamming, eavesdropping and distortion. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to prevent propagation of routing information or worse interrupt messages and distort them to manipulate routes. Routing protocols should be well adopted to handle such problems.

2.4 Problems with existing Ad-hoc routing protocols.

2.4.1 Implicit trust relationship between neighbors. Current Ad-hoc routing protocols inherently trust all participants. Most Ad-hoc routing protocols are cooperative by nature and depend on neighboring nodes to route packets. This naive trust model allows malicious nodes to paralyze an Ad-hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. While these attacks are possible in fixed network as well, the Ad-hoc environment magnifies this makes detection difficult.

2.4.2 Throughput. Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem. Although the average loss in throughput due to misbehaving nodes is not too high, in the worst case it is very high.

2.4.3 Attacks using modification of protocol fields of messages. Current routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Routing protocol packets carry important control information that governs the behavior of data transmission in Ad-hoc networks. Since the level of trust in a traditional Ad-hoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious nodes can easily cause redirection of network traffic and DOS attacks by simply altering these fields.

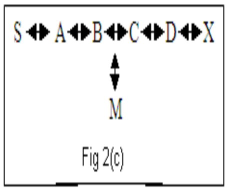

Fig 2(c)

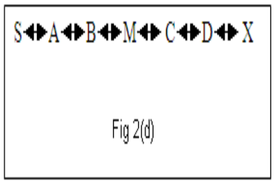

Fig 2(d)

For example, in the network illustrated in Figure 2(c), a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X, which C is advertising.

3. ATTACKS AT THE ROUTING LEVEL IN MANET.

These attacks may have the aim of modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. An attack may also aim at impeding the formation of the network, making legitimate nodes store incorrect routes, and more generally at perturbing the network topology. Let us look at them now.

3.1 Remote Redirection Attacks.

3.1.1 Remote redirection with modified route sequence number (Blackhole Attack). Remote redirection attacks are also called *black hole attacks*. In the attacks, a malicious node uses routing protocol to advertise itself as the shortest path to nodes whose packets it wants to intercept. Protocols such as AODV instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes towards a specific destination. In AODV, any node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value.

Figure 2(c) illustrates an example ad hoc network. Suppose a malicious node, M, receives the RREQ that originated from S for destination X after it is re-broadcast by B during route discovery. M redirects traffic towards itself by unicasting to B a RREP containing a significantly higher destination sequence num for X than the authentic value last advertised by X.

3.1.2 Redirection with modified hop count. A redirection attack is also possible in certain protocols, such as AODV, by modification of the hop count field in route discovery messages. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, malicious nodes can attract route towards themselves by resetting the hop count field of the RREP to zero. Similarly, by setting the hop count field of the RREP to infinity, routes will tend to be created that do not include the malicious node.

3.1.3 Replay Attack. As topology changes, old control messages, though valid in the past, describe a topology configuration that no longer exists. An attacker can perform a replay attack by recording old valid control messages and re-sending them, to make other nodes update their routing tables with stale routes. This attack is successful even if control messages bear a digest or a digital signature that does not include a timestamp.

3.1.4 Wormhole attack. The *wormhole attack* [10] is quite severe, and consists in recording traffic from one region of the network and replaying it in a different region. It is carried out by an intruder node *X* located within transmission range of legitimate nodes *A* and *B*, where *A* and *B* are not themselves within transmission range of each other. Intruder node *X* merely tunnels control traffic between *A* and *B* (and vice versa), without the modification presumed by the routing protocol – e.g. without stating its address as the source in the packets header – so that *X* is virtually invisible. This results in an extraneous inexistent *A* - *B* link which in fact is controlled by *X*, as shown in Figure 3(a). Node *X* can afterwards drop tunneled packets or break this link at will. Two intruder nodes *X* and *X*′, connected by a wireless or wired private medium, can also collude to create a longer (and more harmful) wormhole, as shown in Figure 3(b)

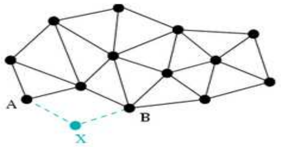

Figure 3(a): A wormhole created by node *X*

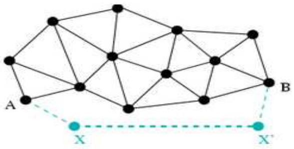

Figure 3(b): A longer wormhole created by two colluding nodes *X* and *X'*.

The severity of the wormhole attack comes from the fact that it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are preserved. Furthermore, on a distance vector routing protocol, wormholes are very likely to be chosen as routes because they provide a shorter path – albeit compromised – to the destination. Marshall [11] points out a similar attack, called the *invisible node attack* by Carter and Yasinsac [12], against the Secure Routing Protocol [13].

3.1.5 Rushing Attack. An offensive that can be carried out against on-demand routing protocols is the *rushing attack* [14]. Typically, on-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. This is done in order to reduce cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker.

Once the malicious node has been able to insert itself between two communicating nodes it is able to do anything with the packets passing between them. It can choose to drop packets to perform a denial of service attack, or alternatively use its place on the route as a first step in man-in-the-middle attack.

3.2 Denial of service attack with modified source routes. DSR is a routing protocol, which explicitly states routes in data packets. These routes lack any integrity checks and a simple denial-of-service attack can be launched in DSR by altering the source routes in packet headers.

Modification to source routes in DSR may also include the introduction of loops in the specified path. Although DSR prevents looping during the route discovery process, there are insufficient safeguards to prevent the insertion of loops into a source route after a route has been salvaged.

3.2.1 Message Bombing. The attacker can also try to perform Denial of Service on the network layer by saturating the medium with a storm of broadcast messages (*message bombing*), reducing nodes' goodput and possibly impeding nodes from communicating. (This is not possible under hybrid routing protocols, where nodes cannot issue broadcast communications [15].) The attacker can even send invalid messages just to keep nodes busy, wasting their CPU cycles and draining their battery power. In this case the attack is not aimed at modifying the network topology in a certain fashion, but rather at generally perturbing the network functions and communications.

3.2.2 Denial of Service Attack over Transport Layer.

(a) Shrew Attack

On the transport layer, Kuzmanovic and Knightly [16] demonstrate the effectiveness of a low-rate DoS attack performed by sending short bursts repeated with a slow timescale frequency (*shrew attack*). In the case of severe network congestion, TCP operates on timescales of Retransmission Time Out (RTO). The throughput (composed of legitimate traffic as well as DoS traffic) triggers the TCP congestion control protocol, so the TCP flow enters a timeout and awaits a RTO slot before trying to send another packet. If the attack period is chosen to approximate the RTO of the TCP flow, the flow repeatedly tries to exit timeout state and fails, producing zero throughput. If the attack period is chosen to be slightly greater than the RTO, the throughput is severely reduced. This attack is effective because the sending rate of DoS traffic is too low to be detected by anti-DoS countermeasures.

(b) Jellyfish Attack

Another DoS performed on the transport layer is the subtle *jellyfish attack* by Aad et al. [17], that deserves particular attention. Its authors point out that, remarkably, it does not disobey the rules of the routing protocol, even if we may argue that, strictly speaking, this is not always the case. But is indeed true that the jellyfish attack is difficult to distinguish from congestion and packet losses that occur naturally in a network, and therefore is hard and resource-consuming to detect.

This DoS attack can be carried out by employing several mechanisms. One of the mechanisms of the jellyfish attack consists in a node delivering all received packets, but in scrambled order instead of the canonical FIFO order. This attack cannot be successfully opposed by the actual TCP packet reordering techniques, because such techniques are effective on sporadic and non-systematic reordering.

The second mechanism is the same as that used in the shrew attack, and involves performing a selective blackhole attack by dropping all packets for a very short duration at every RTO. The flow enters timeout at the first packet loss caused by the jellyfish attack, then periodically re-enters the timeout state at every elapsed RTO.

The third mechanism consists in holding a received packet for a random time before processing it, increasing delay variance. This causes TCP traffic to be sent in bursts, therefore increasing the odds of collisions and losses; it increases the RTO value excessively; and it causes an incorrect estimation of the available bandwidth in congestion control protocols based on packet delays.

3.2.3 Denial of Service Attack over Physical Layer.

DoS attacks can also be carried over on the physical layer (e.g. jamming or radio interference); in this case, they can be dealt with by using physical techniques e.g. spread spectrum modulation [18].

3.3 Attacks using impersonation. A malicious node can launch many attacks by altering its MAC or IP address. Both AODV and DSR are susceptible to this attack.

3.4 Attacks using fabrication. Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

3.4.1 Falsifying route error messages in AODV or DSR. AODV and DSR implement path maintenance measures to recover broken paths when nodes move. If the destination node or an intermediate node along an active path moves, the node upstream of the link break broadcasts a route error message to all active upstream neighbors.

Table 1: Routing Attacks in MANET

Type	Routing Attacks in MANET	Attack Procedure	Remarks
RRA[1]	Blackhole Attack	Malicious node advertises itself as having a valid route, then consumes the intercepted packets.	Wormhole Attack is effective in spite of encryption and digital signatures ,hence the most severe amongst all.
	Redirection with modified hop count	Modifies hop count field in route discovery messages, determine shortest path	
	Replay Attack	Records old valid control messages , re-sends them to make other nodes update their routing tables with stale routes.	
	Wormhole Attack	Records traffic from one region of the network and replays it in different region	
	Rushing Attack	If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker.	
DoS[2]	Message Bombing	By saturating the medium with a storm of broadcast messages	Jellyfish attack is high resource-consuming ,hence hard to detect amongst all.
	Shrew Attack	By sending short bursts repeated with a slow timescale frequency	

	Jellyfish Attack	Three Mechanisms: (a) Node delivers all received packets in scrambled order instead of the canonical FIFO order. (b) Same as that in the shrew attack, involves performing a selective blackhole attack by dropping all packets for a very short duration at every RTO. (c) Holds received packet for a random time before processing it, increases delay variance.	
AuI[3]		Alters MAC or IP address.	
AuF[4]	Falsifying Route Error Message	If destination node or an intermediate node along an active path moves, node also invalidates the route for this destination in its routing table, then by sending false route error messages.	Comparable difficulty in detection
	Route cache poisoning	When information stored in routing table at routers is deleted, altered or injected with false information.	
	Routing Table Overflow	Attacker attempts to create route to non-existent nodes,	

		prevents new routes from being created or overwhelm the protocol.	

1. RRA: Remote Redirection Attack
2. DoS: Denial of Service
3. AuI: Attacks using Impersonation
4. AuF: Attacks using Fabrication

The node also invalidates the route for this destination in its routing table.
The vulnerability is that routing attacks can be launched by sending false route error messages. Suppose node S has a route to node X via nodes A, B, and C, as in Figure3.3. A malicious node M can launch a denial of service attack against X by continually sending route error messages to B spoofing node C, indicating a broken link between nodes C and X. B receives the spoofed route error message thinking that it came from C. B deletes its routing table entry for X and forwards the route error message on to A, who then also deletes its routing table entry. If M listens and broadcasts spoofed route error messages whenever a route is established from S to X, M can successfully prevent communications between S and X.

3.4.2 Route cache poisoning in DSR. This is a passive attack that can occur in DSR due to promiscuous mode of updating routing table which is employed by DSR. This occurs when information stored in routing table at routers is deleted, altered or injected with false information.
In addition to learning routes from headers of packets, which a node is processing along a path, routes in DSR may also be learned from promiscuously received packets. A node overhearing any packet may add the routing information contained in that packet's header to its own route cache, even if that node is not on the path from source to destination.
The vulnerability is that an attacker could easily exploit this method of learning routes and poison route caches. Suppose a malicious node M wanted to poison routes to node X. If M were to broadcast spoofed packets with source routes to X via itself, neighboring nodes that overhear the packet transmission may add the route to their route cache.

3.4.3 Routing table overflow attack. In routing table overflow attack, the attacker attempts to create route to non-existent nodes. The goal of the attacker is to create enough routers to prevent new routes from being created or overwhelm the protocol. Proactive routing algorithms attempt to discover routing information even before they are needed, while reactive algorithms create only when they are needed. This makes proactive algorithms more vulnerable to table overflow attacks. Thus, the main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack

[7]. There are some attacks against routing that have been studied and well known [3] [4] [5] [6]:

- 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.

4 CONCLUSION

In this paper various routing attacks of MANETs are discussed. Misbehaving nodes can affect network throughput adversely in worst-case scenarios. It is necessary to clearly define misbehaving nodes in order to prevent false positives. It may be possible that a node appears to be misbehaving when it is actually encountering temporary problem such as overload or low battery. A routing protocol should be able to identify misbehaving nodes and isolate them during route discovery operation.

REFERENCES

[1] Elizabeth M. Royer, and Chai-Keong Toh, “A Review of Current Routing Protocols.

[2] Charles E. Perkins, and Elizabeth M. Royer, “Ad-hoc On-Demand Distance Vector (AODV) Routing,” Internet Draft, November 2002.

[3] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, San Antonio, TX, January 2002.

[4] Y. Hu, A. Perrig and D. Johnson, Ariadne: “A Secure On-demand Routing Protocol for Ad Hoc Networks”, in *Proceedings of ACM MOBICOM’02,* 2002.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A SecureRouting Protocol for Ad Hoc Networks”, in *Proceedings of ICNP’02,* 2002.

[6] Y. Hu, D. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks”, *Ad Hoc Networks,* 1 (1): 175–192, July 2003.

[7] Yongguang Zhang and Wenke Lee, Security in “Mobile Ad-Hoc Networks”, in Book *AdHoc Networks Technologies and Protocols (Chapter 9),* Springer, 2005.

[8] David B. Johnson, and David A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[9] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Computer Communications Review, pp. 234-244,October 1994.

[10] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. “Packet leashes: A defense against wormhole attacks in wireless ad hoc networks”. In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, CA, USA, April 2003.

[11] John Marshall. “An analysis of SRP for mobile ad hoc networks”. In Proceedings of the 2002 International Multiconference in Computer Science, Las Vegas, USA, August 18–21 2002.

[12] Stephen Carter and Alec Yasinsac. Secure Position Aided Ad hoc Routing. In Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN ’02), pages 329–334, November 4–6 2002.

13] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, USA, January 27–31 2002.

[14] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. “Rushing attacks and defense in wireless ad hoc network routing protocols”. In Proceedings of the 2003 ACM Workshop on Wireless Security, pages 30–40, San Diego, CA, USA, 2003. ACM Press.

[15] Srđan Čapkun, Jean-Pierre Hubaux, and Markus Jacobsson. “Secure and privacy-preserving communication in hybrid ad hoc networks”. Technical Report IC/2004/10, Swiss Federal Institute of Technology Lausanne (EPFL), Lausanne, Switzerland and RSA Laboratories, Bedford, MA, USA, 2004.

[16] Aleksandar Kuzmanovic and Edward W. Knightly. “Low-rate TCP-targeted Denial of Service attacks (The shrew vs. the mice and elephants)”. In Proceedings of the 2003 Conference of the Special Interest Group on Data Communication (SIGCOMM ’03), pages 75–86, Karlsruhe, Germany, 2003. ACM Press.

[17] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly. “Denial of Service resilience in ad hoc networks”. In Proceedings of the 10th Annual International Conference on Mobile

Computing and Networking (MobiCom '04), Philadelphia, Pennsylvania, USA, September 26–October 1 2004.

[18] Raymond L. Pickholtz, Donald L. Schilling, and Laurence B. Milstein. "Theory of spread spectrum communications – a tutorial". IEEE Transactions on Communications, 30(5):855–884, May 1982.