International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 9 (September '2016)

# A STUDY ON ATTACKS AND SECURITY OF MANET ROUTING PROTOCOLS IN MALICIOUS ENVIRONMENTS

**S.Vaitheki,**
M.Phil Scholar,
Department of Computer Science,
Siri PSG College of Arts and Science for women,
Sankari, Tamilnadu, India.

**K.Sudha,**
Assistant Professor,
Department of Computer Science,
Siri PSG College of Arts and Science for women,
Sankari, Tamilnadu, India.

**Abstract:** The nodes in an ad hoc network communicate using wireless links which are by nature vulnerable to interference and channel errors that may corrupt some or many data packets. Moreover, the nodes share the physical medium, compete to transmit data packets and suffer collisions. Thus, one of the problems in detecting malicious nodes that drop packets is that it may not be clear as to whether the packet was dropped due to channel errors, collisions, or due to malicious intent. In most detection mechanisms, the number of packets that are not forward is recorded by a passive listener. In this paper we discussed attacks of MANET.

***Keywords: Wireless nodes, security, attacks, packet dropper, malicious nodes***

## I.INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Such a network may operate in a standalone fashion, or may be connected to the Internet. Key features of MANETs summarized as; No Fixed Infrastructure, Dynamic Topology, Power and Processing Constraints, Intermittent Connectivity, Varying Security Requirements, Scarce Bandwidth and High-Loss, Unreliable Links. Multihop, mobility, large network size combined with device heterogeneity, bandwidth, and battery power constraints make the design of adequate routing protocols a major challenge. The design goal for ad hoc network routing protocols are Minimal control overhead, Minimal processing overhead, Multihop routing capability, Dynamic topology maintenance, Loop prevention, Centralized vs. distributed approaches, Optimal route, Scalability, and Efficiency [1]. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. The network layer security designed for MANETs are concerned with protecting the network functionality to deliver packets between mobile nodes through multihop ad hoc forwarding. Therefore, they seek to ensure that the routing message exchanged between nodes is consistent with the protocol specification, and the packet forwarding behaviour of each node is consistent with its routing states

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. 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. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

Wireless ad-hoc network have many advantages:

- Low cost of deployment: Ad hoc networks can be deployed on the fly; hence no expensive infrastructure such as copper wires or data cables is required.
- Fast deployment: Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Deployment time is shortened.
- Dynamic Configuration: Ad hoc network configuration can change dynamically over time. When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

## II.LITERATURE REVIEW

***Divecha et al.*** [2] have carried out the performance analysis of DSDV and DSR protocols and compared their performances with different mobility models. They concluded that the routing protocols are specific to particular mobility models.

***Ramesh et al.*** [3] have proposed a method to reduce the end to end delay in the multi-path routing protocol by proposing a congestion aware multi-path DSR protocol. It enhances the performance of DSR protocol in congested network. The proposed protocol was compared with ordinary DSR protocol and the results show that the proposed scheme greatly reduces the end to end delay and improves the overhead.

***Williams and Camp*** [4] have presented a comprehensive comparison between different broadcasting schemes used in MANETs. In their paper, they categorized different

 

broadcasting schemes and compared them through simulations, which established various network failures under different conditions like bandwidth consumption, dynamic topologies, and battery consumption. They have also proposed some protocols extension that can adapt to the changing network conditions and improve the functioning of the broadcasting scheme.

***Adibi and Agnew*** [5 in their paper presented a survey on different versions of DSR, pointed out their differences and compared them. The authors have also proposed a multilayer flavored DSR protocol which obtains the information from physical, MAC and network layer and passes this information to the network layer. Then they select the most optimal routing protocol by performing a comparison between the current network condition and the pre-defined closest group of conditions.

***Pirzada and McDonald*** [6] present a method to improve the DSR protocol. They propose the method of deploying trust gateways to reinforce the DSR protocol. In this method, the number of malicious nodes in the network is identified and with the use of the trust gateways, they are avoided in the future exchange of data packets.

***Yong et al.,***[7] trust among nodes is calculated using a combination of direct and indirect trust. When the trust value of a node declines so much that it falls below a threshold, it is then added to a blacklist. The packets from the blacklisted nodes are not forwarded.

***Dhurandher and Mehra*** [8] have employed a message trust based solution to the multipath routing scenario. In this proposed solution each node is initially given a zero trust value indicating an unknown trust level. Based on the behavior of the nodes the assigned trust value is either incremented or decremented. Trust values may be positive, negative or zero, indicating known, malicious, or unknown behavior.

***Mangrulkar and Atique*** [9] presented a scheme that enhances the AODV protocol by adding an extra field in the RREQ called Trust Value. The initial trust value is assigned by the source when it broadcasts RREQ packet. When it receives RREP from the destination it increments the trust value of all the nodes that fall on the route of destination. By adding this extra field the source selects a valid route that has higher trust value rather than selecting the shortest or the longest route. This avoids the disruption of the network as most of the attacks are coordinated on the shortest route to the destination.

## III.SECURITY AWARE ROUTING PROTOCOLS

MANETs have certain unique characteristics that make them vulnerable to several types of attacks. Since they are deployed in an open environment where all nodes co-operate in forwarding the packets in the network, malicious nodes are difficult to detect. Hence, it is relatively difficult to design a secure protocol for MANET, when compared to wired or infrastructure-based wireless networks. This section discusses the security goals for an ad hoc network. Sample attacks and threats against existing MANET routing protocols are then discussed. I then discuss the working of two secure routing protocols to address these threats, ARIADNE [1] and SAODV [2].

### A) Security Services

To secure the routing protocols in MANETs, researchers have considered the following security services: availability, confidentiality, integrity, authentication and non-repudiation [10].

**Availability** guarantees the survivability of the network services despite attacks. A Denial-of-Service (DoS) is a potential threat at any layer of an ad hoc network. On the media access control layer, an adversary could jam the physical communication channels. On the network layer disruption of the routing operation may result in a partition of the network, rendering certain nodes inaccessible. On higher levels, an attacker could bring down high-level services like key management service.

**Confidentiality** ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications. Routing information must also remain confidential in some cases, because the information might be valuable for enemies to locate their targets in a battlefield.

**Integrity** ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

**Authentication** enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information.

**Non-repudiation** ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

The networking environment in wireless schemes makes the routing protocols vulnerable to attacks ranging from passive eavesdropping to active attacks such as impersonation, message replay, message littering, network partitioning, etc. Eavesdropping is a threat to confidentiality and active attacks are threats to availability, integrity, authentication and non-repudiation. Nodes roaming in an ad hoc environment with poor physical protection are quite vulnerable and they may be compromised. Once the nodes are compromised, they can be used as starting points to launch attacks against the routing protocols.

### B) Attacks and exploits on the existing protocols

In general, the attacks on routing protocols can generally be classified as routing disruption attacks [11] and resource consumption attacks [12]. In routing disruption attacks, the attacker tries to disrupt the routing mechanism by routing packets in wrong paths; in resource consumption attacks, some non-cooperative or selfish nodes may try to inject false packets in order to consume network bandwidth. Both of

these attacks are examples of Denial of Service (DoS) attacks. Figure 1 depicts a broader classification of the possible attacks in MANETs.

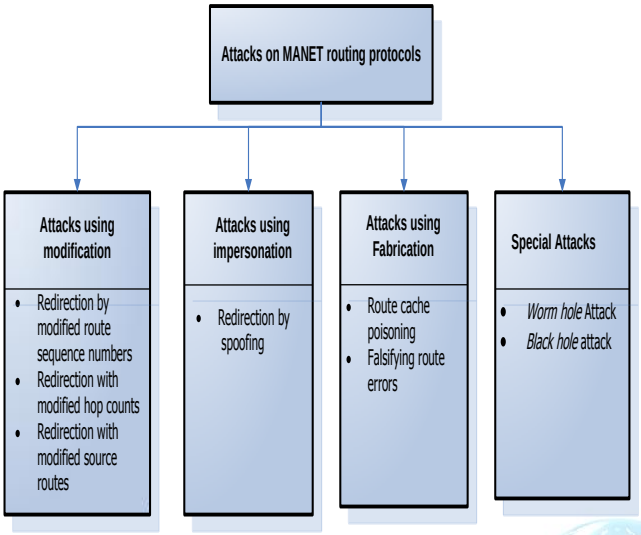


**Figure 1: Classification of attacks on MANET routing protocols**

**Attacks using Modification:** In this type of attacks, some of the protocol fields of the messages passed among the nodes are modified, thereby resulting in traffic subversion, redirection or Denial of Service (DoS) attacks. The following sections discuss some of these attacks.

- **Modification of route sequence numbers:** This attack is possible against the AODV protocol. The malicious node can change the sequence number in the route request packets or route reply packets in order to make the route fresh. In Figure 2, malicious node M receives a route request RREQ from node B that originates from node S and is destined for node X. M unicasts a RREP to B with a higher destination sequence number for X than the value last advertised by X. The node S accepts the RREP and then sends the data to X through M. When the legitimate RREP from X gets to S, if the destination number is less than the one advertised by M, then it will be discarded as a stale route. The situation will not be corrected until a valid RREP with higher sequence number than that of M gets to S.
- **Modification of hop count:** This type of attacks is possible against the AODV protocol in which a malicious node can increase the chance that they are included in a newly created route by resetting the hop count field of a RREQ packet to a lower number or even zero. Similar to route modification attack with sequence number, the hop count field in the routing packets is modified to attract data traffic.
- **Modification of source route:** This attack is possible against DSR which uses source routes and works as follows. In Figure 2, it is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the list and forwards it to C. C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.

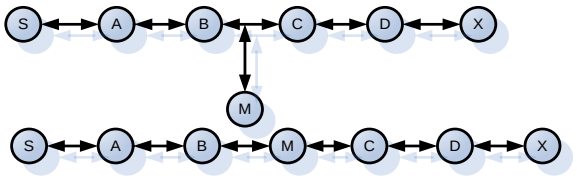


**Figure 2: An example of route modification attack**

**Attacks using Impersonation:** This type of attacks violates authenticity and confidentiality in a network. A malicious node can impersonate or spoof the address of another node in order to alter the vision of the network topology as perceived by another node. Such attacks can be described as follows in Figure 3. 3

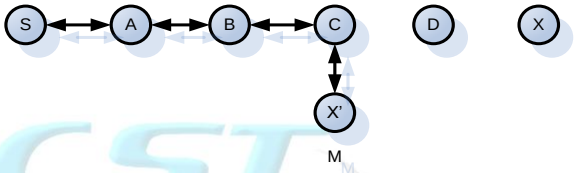


**Figure 3: An example of impersonation attack**

Node S wants to send data to node X and initiates a Route Discovery process. The malicious node M, closer to node S than node X, impersonates node X as X'. It sends a route reply (RREP) to node S. Without checking the authenticity of the RREP, node S accepts the route in the RREP and starts to send data to the malicious node. This type of attacks can cause a routing loop within the network.

**Attacks using Fabrication:** In this type of attacks, a malicious node tries to inject fake messages or routing packets to disrupt the routing mechanism. These attacks are difficult to detect in a MANET since the routing packets appear to be legitimate packets to the nodes processing them. Attacks by fabrication are discussed in [12] and [11]. Figure 4 is an example of fabrication attacks. Node S wants to send data to node X, so it broadcasts a route request in order to find the route to node X. Malicious node M pretends to have a cached route to the destination X, and returns route reply to the source node (S). The source node, without checking the validity of the RREP, accepts the RREP and starts to send data through M. Furthermore, malicious nodes can fabricate RERR to advertise a link break to a certain node in a MANET with AODV or DSR protocols.

**Special Attacks:** In addition to the attacks described above, there are two other severe attacks which are possible against routing protocols such as AODV and DSR.

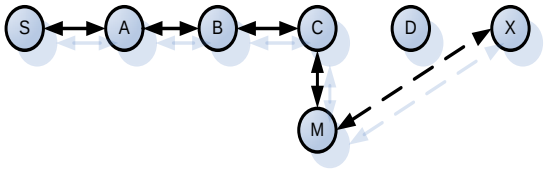


**Figure 4: An example of fabrication attack**

**Wormhole Attack:** The wormhole attack [13] is a severe type of attacks in which two malicious nodes can forward packets through a private "*tunnel*" in the network as shown in Figure 5.

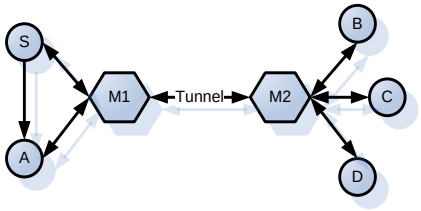


**Figure 5: An example of wormhole attack**

Here, $M_1$ and $M_2$ are two malicious nodes which link through a private connection. Every packet that $M_1$ receives from the network is forwarded through "*wormhole*" to node $M_2$, and vice versa. This attack disrupts routing protocols by short circuiting the normal flow of routing packets. Such a type of attack is difficult to detect in a network, and may severely damages the communication among the nodes. Such an attack can be prevented by using *packet leashes* which authenticate the timing information in the packets to detect faked packets in the network.

**Black hole attack:** A node advertises a zero metric for all destinations causing all nodes around it to route data packets towards it. The AODV protocol is vulnerable to such an attack. This type of attack is described in detail in [7]. After a discussion of the attacks and exploits in the routing protocols, the next section discusses two secure routing protocols for ad hoc wireless networks.

## III.EXPERIMENTAL RESULTS

### Experiments in the benign environment

In this phase, the performance data of four routing protocols (DSR, ARIADNE, AODV and SAODV) are collected. A scenario is set up for data collection. This scenario is run 11 times with 11 different values of the mobility pause time ranging from 0 to 100 seconds. The data is collected according to two metrics, Packet Delivery Fraction and Normalized Routing Load. In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs. The average values of these 11 simulation runs are then calculated for the two metrics and used as a baseline to evaluate the performance of routing protocols in malicious environments.

As shown in Figure 6, the percentage of packets delivered in AODV and SAODV is fairly close to each other, and both methods exhibit superior performance (~90% in general).The security features in SAODV lower the performance a little bit. Actually, the generation and verification of digital signatures depends on the power of the mobile nodes and causes a delay in routing packet processing.

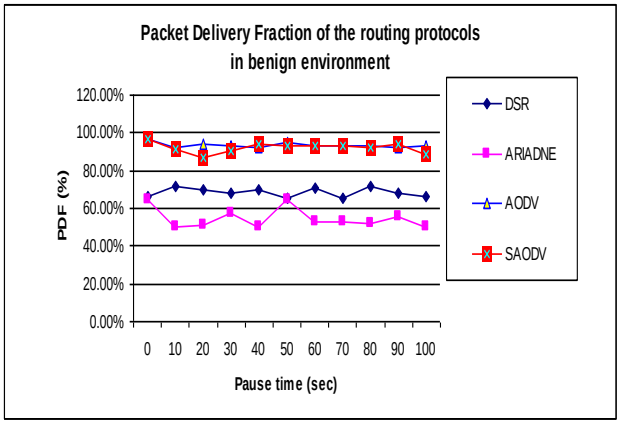


**Figure 6: Packet Delivery Fraction vs. pause time values in benign environment**

In the simulation environments, this delay depends on the simulation running machine and is not high enough to make the significant difference for the PDF metric. On the other hand, the packet delivery fraction in DSR and ARIADNE are 20-40% lower than that of AODV/SAODV across the board given different mobility pause times.

The major difference between AODV and DSR is caused by difference in their respective routing algorithms. It was reported by other researchers that, in high mobility and/or stressful data transmission scenarios, AODV outperforms DSR. The reason is that DSR heavily depends on the cached routes and lack any mechanism to expire stale routes. In the benign environment of our experiments, the default expiry timer of cached route for DSR and ARIADNE is 300 seconds, while this number is 3 seconds for AODV and SAODV. In respect to the protocol design, these values are kept unchanged through all the simulation scenarios. Furthermore, DSR and ARIADNE store the complete path to the destination. The situation is even worse for ARIADNE, mainly because ARIADNE relies on the delayed key disclosure mechanism of TESLA when authenticating packets, including the RERR packets. When an intermediate node in ARIADNE notices a broken link, it sends a RERR message to the source node of the data packet. The source node, however, simply saves the RERR message, because it has not yet received from the intermediate node the key needed to authenticate the route error. The source node keeps sending the data until the second route error is triggered, and another RERR is received. Only then would the previous route error be authenticated, and the broken link not be used any more. This explains the worse performance of ARIADNE in comparison with DSR and other protocols. As shown in Figure 7, the NRL metric is, in general, inversely

proportional to the PDF metric (Figure 6). A low PDF value (for example, ARIADNE in Figure 6) corresponds to a high NRL value (Figure 7).

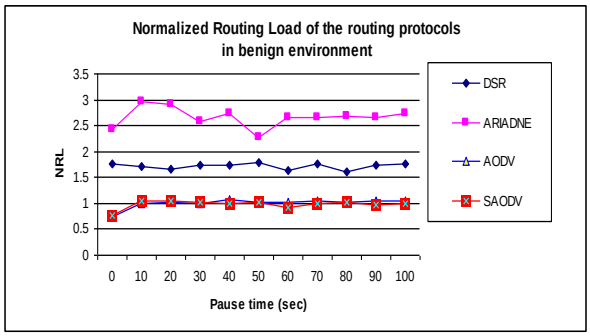


**Figure 7: Normalized Routing Load vs. pause time values in benign environment**

This relationship between PDF and NRL is further illustrated in Table 1, which lists the average values of the two metrics over 11 simulation runs for each of the four protocols.

| Pause Time (seconds) | Packet Delivery Fraction (%) | Normalized Routing Load |
|---|---|---|
| DSR | 68.41% | 1.72 |
| ARIADNE | 54.70% | 2.58 |
| AODV | 93.45% | 1.01 |
| SAODV | 92.00% | 0.98 |

Table 1: The "*baseline*" metrics of the four protocols

The comparison between the normal routing protocols (DSR and AODV) and their respective secure version (that is, ARIADNE and SAODV) in benign environments has been extensively conducted by other researchers .

## IV.CONCLUSION

The attack models are used to make malicious wireless nodes and create various malicious environments, in which the performance of DSR, AODV, ARIADNE, and SAODV are evaluated. With three different attack models for each of the protocols, and with the number of malicious nodes varying from one to five.

## V.REFERENCES

[1]. C. E. Perkins. Ad Hoc Networking. Addison-Wesley Professional, first edition, 2000.

[2]. Bhavyesh Divecha, Ajith Abraham, Crina Grosan. Sugata Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models", First Asia International Conference on Modeling and Simulation, AMS2007. March, 27-30, 2007, Phuket, Thailand. Publisher: IEEE Press, pp. 224-229.

[3]. V. Ramesh, P. Subbaiah, N. Sandeep Chaitanya, K. Sangeetha Supriya, "Performance Comparison of Congestion Aware Multi-Path Routing (with Load Balancing) and Ordinary DSR", 2010 IEEE 4th International Conference on Internet Multimedia Services Architecture and Application(IMSAA),Dec. 15-17, 2010, pp.1-5.

[4]. Brad Williams, Tracy Camp, "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks", MOBIHOC'02, June 9-11, 2002, EPFL, Lausanne, Switzerland, pp. 194-205.

[5]. S. Adibi, G.B. Agnew, "Multi-layer flavored dynamic source routing in mobile ad-hoc networks", IET Communications, 2008, Vol. 2, No. 5, pp. 690–707.

[6]. Asad Amir Pirzada, Chris McDonald, "Deploying Trust Gateways to Reinforce Dynamic Source Routing", 2005 3rd IEEE International Conference on Industrial Informatics, (INDIN '05),Aug. 10-12, 2005, pp. 779- 784.

[7]. CHENG Yong, HUANG Chuanhe, SHI Wenming, "Trusted Dynamic Source Routing Protocol", Wireless Communications, International Conference on Networking and Mobile Computing, WiCom2007, Sept. 21-25 ,2007,pp.1632-1636.

[8]. Sanjay K. Dhurandher, Vijeta Mehra, "Multi-path and Message Trust-Based Secure Routing in Ad Hoc Networks", International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT '09., Dec. 28-29,2009, pp.189-194.

[9]. R. S. Mangrulkar, Mohammad Atique, "Trust Based Secured Ad hoc on Demand Distance Vector Routing Protocol for Mobile Ad Hoc Network", 2010 Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), Dec. 15-19 ,2010,pp.1-4.

[10]. Sandipan Dey, Ajith Abraham, Sugata Sanyal," An LSB Data Hiding Technique Using Prime Numbers", Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (IIHMSP 2007),Kaohsiung City, Taiwan, IEEE Computer Society press, USA,vol.2, Nov. 26-28, 2007, pp.473-476.

[11]. Zhenhui Zhai, Yong Zhang, Mei Song, Guangquan Chen, "A Reliable and Adaptive AODV Protocol based on Cognitive Routing for Ad Hoc Networks", 2010 The 12th International Conference on Advanced Communication Technology (ICACT),Gangwon-Do, Korea, vol.2, Feb. 7-10, 2010, pp.1307-1310,

[12]. C.-K. Toh. "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*". Prentice Hall publishers, December 2001, ISBN 0130078174.

[13]. David B. Johnson David A. Maltz Josh Broch. **"***DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks'.*In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001. http://www.cs.ust.hk/~qianzh/COMP680H/reading-list/johnson01.pdf