Volume 1 No. 4, August 2011 ISSN-2223-4985
International Journal of Information and Communication Technology Research

http://www.esjournals.org

Security Issues in Ad Hoc Networks

Sima
Department of Computer Science & Engg.
Karnal Institute of Technology & Management Kunjpura Karnal (Haryana, India)

ABSTRACT

Mobile ad hoc networks have inherently different properties than traditional wired networks. These new characteristics present different security vulnerabilities and this paper provides a detailed classification of these threats. Threats exist to a mobile ad hoc network both from external nodes unauthorized to participate in the mobile ad hoc networks, and from internal nodes, which have the authorization credentials to participate in the mobile ad hoc network. Internal nodes giving rise to threats can be further divided according to their behavior — failed, badly failed, selfish and malicious nodes. All categories of node behavior should be considered when designing protocols for mobile ad hoc networks.

Keywords: *Security, Ad hoc Networks, Routing Protocols.*

1. INTRODUCTION

An ad-hoc network is a collection of nodes forming a temporary network with out the aid of any additional infrastructure and no centralized control. The nodes themselves are responsible for routing the packets. The nodes in an ad-hoc network can be a laptop, PDA, or any other device capable of transmitting and receiving information. Nodes act both as an end system (transmitting and receiving data) and as a router (allowing traffic to pass through) resulting in multihop routing. Network is temporary as nodes are generally mobile and may go out of range of other nodes in the network. The routing protocol sets an upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. The problem is enlarged by the fact that routing usually needs to rely on the trustworthiness of all the nodes that are participating in the routing process. It is hard to distinguish compromised nodes from nodes that are suffering from bad links. In this paper, various security problems are discussed in the ad hoc networks. The main goal of the security solutions for an Ad Hoc network is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users [1]

2. MOBILE ADHOC ROUTING

Routing is a major area of research in ad hoc networks, as the characteristics of ad hoc networks pose many new challenges by comparison with traditional wired area networks. A routing protocol is needed whenever a packet needs to be handed over via several nodes to arrive at its destination. A routing protocol finds a route for packet delivery and delivers the packet to the correct destination. Routing Protocols have been an active area of research for many years; many protocols have been suggested keeping applications and type of network in view. Routing protocols can broadly classify into two types as (a) Table Driven Protocols or Proactive Protocols and (b) On-Demand Protocols or Reactive Protocols[2]

Whenever a packet wants to move from source to destination then a routing protocol is required that governs the data communication over the network.. Two categories of protocols available are:

2.1 Table-Driven routing protocols (Proactive)

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing. Some of the existing table driven[10] or proactive protocols are: DSDV [4] ,OLSR [5] and ZRP [6].

2.2 On Demand routing protocols (Reactive)

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network. Some popular ones are; DSR[7], LAR1 [8] and AODV [14].

3. AD HOC NETWORK ROUTING THREATS

The main threats to an ad hoc network routing protocol are as follows:

Confidentiality: The primary confidentiality threat in the context of routing protocols is to the privacy of the routing information itself, which leads to a secondary privacy

threat to information such as the network topology, geographical location, etc.

Integrity: The integrity of a network depends on all nodes in the network following correct routing procedures so that every node has correct routing information. Therefore threats to integrity are those which either introduce incorrect routing information or alter existing information.

Availability: This is defined as access to routing information at all times upon demand. If a route exists to a mobile node, then any node should be able to get that route when they require it.

Authorization: An unauthorized node is one which is not allowed to have access to routing information, and is not authorized to participate in the ad hoc routing protocol.

Dependability and reliability: One of the most common applications for ad hoc networks is in emergency situations when the use of wired infrastructure is infeasible.

Accountability: This will be required so that any actions affecting security can be selectively logged and protected, allowing for appropriate reaction against attacks.

4. INTERNAL AND EXTERNAL THREATS

The threat model used here distinguishes between external and internal attacks [15]. External attacks are performed by unauthorized nodes or entities. These threats are likely to be more easily detected than threats from internal nodes.

4.1 External threats

External threats indirectly affect the network.

Two types of External threats are:

Eavesdropping: The attacker monitors transmissions for message content.
Traffic analysis: The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication.

4.2 Internal Threats

The threats posed by internal nodes are very serious, so internal nodes will have the necessary information to participate in distributed operations. Internal nodes can misbehave in a variety of different ways; we identify four categories of misbehavior — failed nodes, badly failed nodes, selfish nodes and malicious nodes.

a) **Failed Nodes:** Failed nodes are simply those unable to perform an operation; this could be for many reasons, including power failure and environmental events. The main issues for ad hoc routing are failing to update data structures, or the failure to send or forward data packets, including routing messages. This is important as those data packets may contain important information pertaining to security, such as authentication data and routing information.

b) **Badly Failed Nodes:** Badly failed nodes exhibit features of failed nodes such as not sending or forwarding data packets or route messages. In addition they can also send false routing messages, which are still correctly formatted, but which contain false information and are a threat to the integrity of the network.

c) **Selfish Nodes:** Selfish nodes exploit the routing protocol to their own advantage, e.g. to enhance performance or save resources. Selfish nodes are typified by their unwillingness to cooperate as the protocol requires whenever there is a personal cost involved, and will exhibit the same behaviours as failed nodes, depending on what operations they decide not to perform.

d) **Malicious Nodes:** Malicious nodes aim to deliberately disrupt the correct operation of the routing protocol, denying network services if possible. Hence, they may display any of the behaviours shown by the other types of failed nodes.

e) **Denial of Service Attacks:** The most common threats lead to a denial of service attack, which in turn induces the ‘sleep deprivation torture’ attack [13].

5. PROTOCOLS SPECIFIC ATTACKS

a) **Attacks on Network Integrity:** Many denial of service attacks are also threats to network integrity, exploiting the routing protocol to introduce incorrect routing information. Another factor is that the more densely populated is the area in which a malicious node attacks, the more nodes will be affected. Protocols such as OLSR use a pure flooding mechanism so false information will be relayed to every node [3]. With the hierarchical FSR protocol, participating nodes far away from the malicious node will be less sensitive to its injected false information, especially in a multi-scopev implementation [11].

b) **Attacking Neighbour Sensing Protocols:** Malicious nodes can either force nodes to incorrectly add neighbours when they do not exist, or cause nodes to ignore valid neighbour nodes. The method will depend on the neighbour sensing protocol but most require the receipt of some form of message. Thus, this attack will be more successful for the malicious

node if it could exploit some other operation such as a blacklist. If a bidirectional MAC4 protocol is in use, DSR uses a blacklist for neighbours a node believes it has asymmetrical links with [9]. Thus, a malicious node could just try to block transmission in one direction to cause the node to be added to its blacklist. Blacklisted entries either expire or are deleted when bi-directional communication has been confirmed. So, conversely, a malicious node could try to force a node to delete neighbours from its blacklist by masquerading as a blacklisted node, and forward a route request, whose source header contains details of the blacklisted node (its IP address etc.). A similar attack can be achieved with AODV [12].

c) **Exploiting Route Maintenance:** Malicious nodes can simply propagate false route error messages so that valid working links are marked as broken. Resources will be used in attempts to repair the links or find alternative routes. An alternative attack may be for a malicious node to coerce another node into sending route error messages by blocking an operational link (e.g. by blocking acknowledgments in DSR [9]. This attack can also be performed by an external attacker.

d) **Attacking Sequence Numbers and Duplicate Mechanism:** Unique sequence numbers prevent replay attacks of old data packets. However, this mechanism can also be exploited to cause a denial of service. A malicious node could flood the network with as many messages with false source addresses containing as many high sequence numbers as possible. This attack is possible because most protocols require nodes to maintain their own sequence number counter, and do not take into account the sequence numbers of received messages. Note that this discussion refers to message identifier sequence numbers and not the sequence numbers used to guarantee route freshness as in AODV and OLSR.

e) **Attacks on Protocol Specific Optimizations:** There are many protocol specific attacks. The following describes an attack on the DSR salvaging operation which is used to find alternative routes when a link break is detected [9]. Using the attacks just described above, the malicious node injects into the network as many routes, with as many different next hops, as possible, all of which do not exist and all point to the same target. The malicious node then sends a data packet addressed for that non-existent target.

6. CONCLUSION

Mobile ad hoc networks present different threats due to their very different properties. These properties open up very different security risks from conventional wired networks, and each of them affects how security is provided and maintained. Some of the types of internal threat identified give rise to different security requirements, several of which apply to ad hoc routing. Any protocols and simulations to test them should include the capability to handle each type of node and attack. The effort will help in standardizing the route selection of MANET and also developing a new strategy for secured routing.

ACKNOWLEDGEMENT

I sincerely thank Dr Ashwani Kush for his valuable guidance in this paper preparation and my research work**.**

REFERENCES

[1] R. Hauser, A. Przygienda and G. Tsudik, “Reducing the cost of security in link state routing”, In Symposium on Network and Distributed Systems Security (NDSS ‟97), San Diego, California, Internet Society, pp 93–99, February 1997.

[2] www.wikipedia.org.

[3] "Wireless Network Industry Report". http : // www.wirelessnets.com/resources/downloads/wireless_industry report_2007.html

[4] Hogie L., Bouvry P., ―An overview of MANETs Simulation‖, Electronic notes in theoretical computer science, © 2006 Elsevier, doi:10.1016/j.entcs.2005.12.025.

[5] Stephanie Demers and Latha Kant, ‘‘Manets: perfrormance analysis and management’’ Telcordia Technologies Inc. One Telcordia Drive, Piscataway, NJ 08854.

[6] Zygmunt J. Haas. A New Routing Protocol for the Reconfigurable Wireless Networks UPC’97, October 1997.

[7] David B. Johnson David A. Maltz Josh Broch, ‘‘DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks’’, *Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891*

[8] Ko, Y.B., & Vaidya, N.H. (1998). Location Aided Routing (LAR) in mobile adhoc network Proceedings of the 4th annual ACM/IEEE International Conference on Mobile Computing and Networking. (MobiCom) ISBN i-58113-035-X (pp.66-75)

[9] D. Johnson, D. Maltz, and J. Broch. DSR the dynamic source routing protocol for multihop wireless ad hoc networks. In C. Perkins, editor,

Ad Hoc Networking, chapter 5, pages 139–172. Addison-Wesley, 2001.

[10] J. Lundberg. Routing security in ad hoc networks. In Heidi Pehu-Lehtonen Helger Lipmaa, editor, Proceedings of the Helsinki University of Technology Seminar on Network Security, Fall 2000, Helsinki, Finland. Helsinki University of Technology, 2000.

[11] G. Pei, M. Gerla, and T-W. Chen. Fisheye state routing: A routing scheme for ad hoc wireless networks. In 2000 IEEE International Conference on Communications, ICC 2000, Global Convergence Through Communications, June 18-22, 2000, New Orleans, USA, volume 1, pages 70–74. Institute of Electrical and Electronics Engineers, IEEE Press, 2000.

[12] C. Perkins and E. Royer. The ad hoc on-demand distance-vector protocol. In C. Perkins, editor, Ad Hoc Networking, chapter 6, pages 173–219. Addison-Wesley, 2001.

[13] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In B. Christianson, B. Crispo, and M. Roe, editors, Security Protocols, 7th International Workshop, April 19-21, 1999, Cambridge, UK, volume 1796 of Lecture Notes in Computer Science, pages 172–194. Springer, 2000.

[14] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, andJ. Jetcheva, “A performance comparison of multi-hop wireless ad hoc network routing protocols,” Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’98), pp. 85-97, Oct. 1998.

[15] L. Zhou and Z. Haas. Securing ad hoc networks. IEEE Network, 13(6):24–30, November 1999.