Attacks against Mobile Ad Hoc Networks Routing Protocols

S. A. Razak, S. M. Furnell, P. J. Brooke
Network Research Group, University of Plymouth
Plymouth, Devon PL4 8AA
Email: info@network-research-group.org

***Abstract*-This paper outlines some important issues that relate to security attacks against mobile ad hoc networks from research carried out at Network Research Group, University of Plymouth, on designing intrusion detection system for mobile ad hoc network. In designing security mechanisms for mobile ad hoc networks, one must consider the attacks variations as well as the characteristics of the attacks that could be launched against the ad hoc networks. The discussions of these two aspects are summarized in this paper. This paper also classifies several common attacks against the ad hoc networks routing protocols based upon the techniques that could be used by attackers to exploit routing messages. Those techniques are modification, interception, fabrication, and interruption.**

I. Introduction

Recent advances in computer networking have introduced a new technology for future wireless communication, a mobile ad hoc network (MANET). This technology, which is the combination of peer-to-peer techniques, wireless communications, and mobile computing, provides convenient infrastructure-less communications and could be very useful to provide communications for many applications especially when the infrastructure networks is not feasible. MANET could be used to overcome geographical constraints in a military operation. As it is easy to deploy, it may also very useful to assist in the disaster relief operations where temporary network infrastructure is immediately needed to replace the damaged infrastructure networks.

However, similar to other networks, MANET also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself [1]. As people will be encouraged to use a secured network, it is important to provide MANET with reliable security mechanisms if we want to see this exciting technology become widely used in a next few years. Before the development of any security measure to secure mobile ad hoc networks, it is important to study the variety of attacks that might be related to such networks. With the knowledge of some common attack issues, researchers might have a better understanding of how mobile ad hoc networks could be threatened by the attackers, and thus might lead to the development of more reliable security measures in protecting them.

The purpose of this study is to investigate some of the important issues that might be related to security attacks in mobile ad hoc networks. In Section II, we see how attacks against the ad hoc networks may vary depending upon in which environment the attacks are launched, what communication layer the attacks are targeting, and what level of ad hoc network mechanisms are targeted. After considering these three variations, it is also important to investigate the characteristics of attacks against the ad hoc networks. This issue is discussed in Section III. In this paper, we give a special attention to attacks that could be launched against the routing protocols. We identified that most of the attacks against ad hoc networks routing protocols are actually launched by exploiting the routing messages, and further classify them based upon the techniques that could be used to exploit routing messages in Section IV. Finally, we conclude our study and present our future work in Section V.

II. Attacks Variations

A. Ad hoc networks environments

Ad hoc network can exist in one of three environments; organized, localized, and open environments. Nodes in all of these environments are generally threatened by the same security problems. However, there are some security problems, that are unique to one environment and need more attention in that environment than the others need. Vast numbers of unstructured nodes and the absence of *a priori* relations are some of the main characteristics of the open environment ad hoc networks. Such networks are quite similar to the localized environment networks, but the larger amount of nodes, and the wider coverage area, renders nodes in the open environment to more sophisticated security attacks than the localized networks do. For instance, nodes in both open and localized environments suffer from the absence of a central authority. However, this is not a big issue in a localized environment, because nodes in that environment might have a physical contact with each other to employ any security measures. Security could also be easily enforced in the organized environment because nodes in that environment are usually pre-employed with appropriate security measures before they participate in any specific tasks such as in a military operation.

B. Communication layers

Each layer in the ad hoc networks communication protocols has its own vulnerabilities. In a physical layer, mobile nodes as well as the communication links are

ISBN: 1-9025-6010-8

vulnerable to both passive and active attacks. Passive eavesdropping, signal jamming, denial of service (DoS) attacks, and physical hardware tampering are among the most popular attacks in this layer [2]. Such attacks could be made less useful by encrypting the communication signal, employing spread-spectrum communication technology, and using a tamper-resistant hardware.

Similar link jamming and DoS attacks are also threatening the ad hoc networks at the data link layer. At this layer, adversaries might jam the communication links by sending huge data to the networks, or by replaying unnecessary packets to exhaust the networks' resources. Expensive cryptography algorithms and more sophisticated security measures could be very useful at this layer to protect the networks and to distinguish between valid and invalid packets traversed in the networks.

Attackers are also threatening the ad hoc networks at both the transport and the application layers. At the transport layer, messages are exchanged on the end-to-end basis using secured routes established in the network layer. For that reason, ensuring security at the network layer is very important to provide reliable communication at the transport layer. Similar to the other types of networks, attackers can always find a loophole in the ad hoc networks' applications and might use this vulnerability to launch attacks at the application layer. However, since similar attacks also occur in the other types of networks, regular solutions used in wired networks could be reused to defend the ad hoc networks against attacks at the application layer.

Besides providing reliable routes to exchange messages in the transport layer, network layer also provides the most critical service in the ad hoc network, which is the routing protocol. Several routing protocols have been introduced to provide reliable communication among nodes, but less attention to the security aspects when designing such protocols has opened many security holes at this layer [3].

C. Attack level

There are two main levels of attack in the ad hoc network; attacks against the basic mechanisms and attacks against the security mechanisms [4]. Ad hoc networks have their own unique basic mechanisms, such as the use of wireless links for communications, employing their own routing strategies, and operate in a distributed manner. All these basic mechanisms are actually reflecting to their own unique characteristics that differentiate them from other types of networks. Attackers might launch many security attacks against these basic mechanisms. For instance, attackers could launch passive eavesdropping attacks against the wireless links, drain off node's limited resources, and launch active attacks to interrupt the routing mechanisms.

Responding to many security attacks against the ad hoc network basic mechanisms, researchers have introduced a number of security measures to protect the networks. However, all these security measures are also vulnerable to attacks and need to be secure. Examples of attacks against security mechanisms are stealing username and password to get unauthorized access in the networks and modifying public key databases to disrupt authentication, confidentiality, and integrity services.

III. ATTACK CHARACTERISTICS

Dynamic topology, distributed operation, and resource constraints are some of the unique characteristics that exist in the ad hoc networks, which inevitably increase the vulnerability of such network. Many characteristics might be used to classify attacks in the ad hoc networks. Examples would include looking at the behaviour of the attacks (passive vs. active), the source of the attacks (external vs. internal), the processing capability of the attackers (mobile vs. wired), and the number of the attackers (single vs. multiple).

A. Passive vs. active attacks

Passive attacks are launched to steal valuable information in the targeted networks. Examples of passive attacks in ad hoc network are eavesdropping attacks and traffic analysis attacks. Detecting this kind of attack is difficult because neither the system resources nor the critical network functions are physically affected to prove the intrusions [5].

While passive attacks do not intend to disrupt the network operations, active attacks on the other hand actively alter the data with the intention to obstruct the operation of the targeted networks. Examples of active attacks comprise actions such as message modifications, message replays, message fabrications and the denial of service attacks.

B. External vs. internal attacks

External attacks are attacks launched by adversaries who are not initially authorized to participate in the network operations. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually initiated by the external attackers.

More severe attacks in the ad hoc networks might come from the second source of attacks, which is the internal attack. Internal attacks are initiated by the authorized nodes in the networks, and might come from both compromised and misbehaving nodes. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the ad hoc networks. Security requirements such as authentication, confidentiality and integrity are severely vulnerable in the ad hoc networks with the compromised internal nodes because communication keys used by these nodes might be stolen and passed to the other colluding attackers. On the other hand, nodes will be classified as misbehaving if they are authorized to access the

system resources, but fail to use these resources in a way they should be [6]. Internal nodes might misbehave to save their limited resources, such as the battery powers, the processing capabilities, and the communication bandwidth. Attacks that are caused by the misbehaving internal nodes are difficult to detect because to distinguish between normal network failures and misbehaviour activities in the ad hoc networks is not an easy task.

C. Mobile vs. wired attackers

Mobile attackers are attackers that have the same capabilities as the other nodes in the ad hoc networks. Since they have the same resources limitations, their capabilities to harm the networks operations are also limited. For instance, with the limited transmitting capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity. They are not capable to launch the network jamming attacks to disrupt the whole networks operations.

On the other hand, wired attackers are attackers that are capable of gaining access to the external resources such as the electricity. Since they have more resources, they could launch more severe attacks in the networks, such as jamming the whole networks or breaking expensive cryptography algorithms. Existence of the wired attackers in the ad hoc networks (especially in the open environment networks) is always possible as long as the wired attackers are able to locate themselves in the communication range and have access to the wired infrastructures.

D. Single vs. multiple attackers

Attackers might choose to launch attacks against the ad hoc networks independently or by colluding with the other attackers. One man action or single attackers usually generate a moderate traffic load as long as they are not capable to reach any wired facilities. Since they also have similar abilities to the other nodes in the networks, their limited resources become the weak points to them [7]. For instance, complex cryptography algorithms could be used to help in defending the authentication, integrity, and the confidentiality services from a single attacker. As it becomes very expensive for the single attackers to break the encrypted messages, nodes in the networks could share the expensive cryptography workloads with each other by exploiting the distributed operations and the multiple connections they had among them.

However, if several attackers are colluding to launch attacks, defending the ad hoc networks against them will be much harder. Colluding attackers could easily shut down any single node in the network and be capable to degrading the effectiveness of network's distributed operations including the security mechanisms. Adding to the severity, colluding attackers could be widely distributed or reside at the certain area where they presumed high communication rate in the networks exist. If no suitable security measures employed, nodes in that targeted area are susceptible to any kind of denial of service (DoS) attacks that could be launched by the colluding attackers.

IV. ATTACKS AGAINST ROUTING MESSAGES

Routing is one of the most vital mechanisms in the ad hoc networks. Improper and insecure routing mechanisms will not only degrade the performance of the ad hoc networks, but will also render such networks vulnerable to many security attacks. One of the basic elements in the routing mechanism is the routing message, which is used to establish and maintain relationships between nodes in the networks. The importance of the routing message has made it a main target by the attackers to launch attacks against the ad hoc networks [3, 8]. Attacks against the routing messages could be launched in many forms and may include all the characteristics described in Section III. In this work, attacks against routing messages are classified based on the classification suggested by Stallings in [9]. In such classification, information or messages could be deviated from the normal operation flow using modification, interception, interruption or fabrication attacks. In a more severe case, attackers also might use any combination of these attacks to disrupt the normal information flow. As far as our concern, this study is the first to address security attacks against the ad hoc networks routing messages.

A. Modification

In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the sporadic relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks. Examples of attacks that can be classified under the message modification attacks are packet misrouting and impersonation attacks.

1) *Packet misrouting attacks*: In a packet misrouting attack, malicious nodes reroute traffic from their original path to make them reach the wrong destinations [10]. Attackers might misroute a packet to make it stay in the network longer than its lifetimes, thus render it to be dropped from the network. As a result, the source node needs to retransmit the lost packets and this will consume more bandwidth, as well as increasing the overhead in the networks.

2) *Impersonation attacks*: The impersonation attacks, also called the spoofing attacks, are attacks where malicious node assumes the identity of another node in the networks [11]. By impersonating another node, attackers are able to receive routing messages that are directed to the nodes they faked.

Impersonation attacks are possible in the ad hoc networks because most of the current ad hoc routing protocols do not authenticate the routing packets. As a result, malicious nodes might exploit this loophole to masquerade as another node by modifying the contents of the packets.

B. Interception

Attackers might launch the interception attacks to get an unauthorized access to the routing messages that are not intentionally sent to them. This kind of attack jeopardizes the integrity of the packets because such packets might be modified before being forwarded to the next hop. Besides, the intercepted packets might also be analysed before passed to the destination thus violating the confidentiality. Examples of attacks that can be classified under the interception attacks are wormhole attacks, black hole attacks, and routing packet analysis attacks.

1) *Wormhole attacks*: In the wormhole attacks, a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two colluding attackers are usually transmitted using wired connection to create the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations.

2) *Black hole attacks*: In this attack, malicious nodes trick all their neighbouring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighbouring nodes as having the most optimal route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighbouring node, in the black hole attacks, only one attacker is involved and it threatens all its neighbouring nodes.

3) *Routing packet analysis attacks*: Since no disruptive action occurs, routing packet analysis could be classified as one of the passive attacks against the ad hoc networks. One way to launch this attack is by exploiting the *promiscuous* mode employed in the ad hoc network. In a *promiscuous* mode, if node A is the neighbour of both nodes B and C at a particular time, node A can always hear the transmissions between node B and node C. By exploiting this nature, node A is able to analyze the overheard packets transmitted between node B and node C. More explanation regarding the *promiscuous* mode in the ad hoc networks can be found in [12]. Besides, malicious nodes could also launch this attack by exploiting the nature in a multi hop routing. In multi hop routing, packets need to be forwarded through several intermediate nodes before reaching the actual destination. Malicious nodes might exploit this opportunity by locating themselves in any location along the route to participate in the message forwarding process and later launch the routing packet analysis attacks.

C. Fabrication

Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause chaos in the network operations. They could launch the message fabrication attacks by injecting huge packets into the networks such as in the sleep deprivation attacks. However, message fabrication attacks are not only launch by the malicious nodes. Such attacks also might come from the internal misbehaving nodes such as in the route salvaging attacks.

1) *Sleep deprivation attacks*: This kind of attack is actually more specific to the mobile ad hoc networks. The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets. For instance, attackers could flood any node in the networks by sending a huge number of route request (RREQ), route replies (RREP) or route error (RERR) packets to the targeted node. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the networks.

2) *Route salvaging attacks*: Route salvaging attacks are launched by the greedy internal nodes in the networks. In a mobile ad hoc network, there is no guarantee that each transmitted packet will successfully reach the desired destination node [13]. Packets might not reach the destination node because of the natural network failures or might be under attacks by the adversaries. Therefore, to salvage their packets from such failures, misbehaving internal nodes might duplicate and retransmit their packets although no sending error messages received. The effects of the route salvaging attacks might be more severe if there are many greedy nodes in the networks. Besides draining off more resources in intermediate and destination nodes, this attack might also cause the consumption of unnecessary bandwidth.

D. Interruption

Interruption attacks are launched to deny routing messages from reaching the destination nodes. Adversaries could do this by either attacking the routing messages or attacking the mobile nodes in the networks. Actually, most of the attacks launched in the modification, interception, and fabrication attacks are aimed to interrupt the normal operations of the ad

hoc networks. For instance, adversaries aiming to interrupt the availability service in the networks might destroy all paths to a particular victim node by using the message modification attacks. In a message fabrication attack, adversaries could overload the networks by injecting huge unnecessary packets. Examples of attacks that could be classified under the interruption attacks category are packet dropping attacks, flooding attacks, and lack of cooperation attacks.

1) *Packet dropping attacks*: Direct interruption to the routing messages could be done by using the packet dropping attacks. In a standard packet dropping attack, an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attacks if it is included as one of the intermediate nodes. In addition, instead of constantly dropping all the packets, adversaries might vary their techniques using random, selective, or periodic packet dropping attacks to help their interrupting behaviour remain concealed [14].

2) *Flooding attacks*: Adversaries also might interrupt the normal operations in the packet forwarding process by flooding the targeted destination nodes with huge unnecessary packets. Nodes under the flooding attacks are unable to receive or forward any packet thus all the packets directed to them will be discarded from network.

3) *Lack of cooperation attacks*: Lack of cooperation from the internal nodes to participate in the network operations can also be seen as an attempt to launch a refusal of service attack. In such attacks, internal nodes are discouraged to cooperate in the network operations that did not benefit them because participating in such operations will drain off their resources. Misbehaving internal nodes might use different strategies to save their limited resources. They might refuse to forward the other node's packets, not send back the route error report to the sender when failing to forward packets, or might turn off their devices when not sending any packet in the networks.

V. Conclusions

In this paper, one can see that attacks against the ad hoc networks may vary depend on (1) which environment the attacks are launched, (2) what communication layer the attacks are targeting, and (3) what level of ad hoc network mechanisms are targeted. One can also see that there are several attack characteristics that must be considered in designing any security measure for the ad hoc network. By investigating the characteristics and variations of the attacks, one can make a long list of attacks that could be launch against the ad hoc networks. However, since this study is focusing on the vulnerabilities of the ad hoc networks routing protocols, only some of the common attacks that could be launched against the ad hoc network routing protocols have been investigated. From the investigation, we identified that most of the common attacks against the ad hoc networks routing protocols are actually launched by exploiting the routing messages. From there, we further classify attacks against the routing protocols based upon the techniques that could be used by the attacker to exploit routing messages. In a future work, several security solutions that have been proposed to secure routing protocols will be investigated and classified based on this classification. The investigation will include various techniques that might be employed in protecting, detecting, and responding to the attacks against the routing messages.

VI. References

[1] T. Karygiannis and L. Owens, "Wireless Network Security, 802.11, Bluetooth and Handheld Devices," *NIST Publication*, p. 800(48), November 2002.

[2] J. Al-Jaroodi, "Security Issues in Wireless Mobile Ad Hoc Networks at the Network Layer," University of Nebraska-Lincoln, Dept. of Computer Science and Engineering, Technical Report TR02-10-07, November 2002.

[3] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in Proc. of 2002 IEEE International Conference on Network Protocols (ICNP), pp. 778-89, Nov. 12-15, 2002.

[4] J. P. Hubaux, L. Buttyan, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," in *Proc. of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHOC 2001*, pp. 146-155, Oct. 4-5, 2001.

[5] S. Bouam and J. B. Othman, "Data Security in Ad hoc Networks using MultiPath Routing," in *Proc. of the 14th IEEE PIMRC*, pp. 1331-1335, Sept. 7-10, 2003.

[6] S. Ghazizadeh, O. Ilghami, E. Sirin, and F. Yaman, "Security-Aware Adaptive Dynamic Source Routing Protocol," In *Proc. of 27th Conference on Local Computer Networks*, pp. 751-760, Nov. 6-8, 2002.

[7] G. Schäfer, "Research Challenge in Security for Next Generation Mobile Networks," *Position Papers PAMPAS '02 - Workshop on Requirements for Mobile Privacy & Security*, Sept. 16-17, 2002.

[8] H. Li, Z. Chen and X. Qin, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks," Univ. of Kentucky, Department of Computer Science, Term-paper, 2003.

[9] W. Stallings, *Cryptography and network security*, *Principles and practice, 2nd ed.*, Prentice Hall, Inc, 1999, pp. 6-9.

[10] S. Rajavaram, H. Shah, V. Shanbhag, J. Undercoffer, and A. Joshi, "Neighborhood Watch: An Intrusion Detection and Response Protocol for Mobile Ad Hoc Networks," Student Research Conference, University of Maryland at Baltimore County (UMBC), May 3, 2002.

[11] A. Burg, "Ad hoc networks specific attacks," Technische Universität München, Institut für Informatik, Seminar Paper, Seminar Ad Hoc Networking: concept, applications, and security, Nov., 2003.

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. of the 6th annual international conference on Mobile computing and networking*, pp. 255-265, Aug. 6-11, 2000.

[13] S. Y. Ni, Y. C. Tseng, Y. S. Chen, and J. P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proc.*

of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp. 151-162, Aug. 15-19, 1999.

[14] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies," in *Proc. of The 23rd International Conference on Distributed Computing Systems (ICDCS)*, pp. 478-489, May 19-22, 2003.