IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

The Module Description for Prevention of Attacks to Make MANET More Secure

Narender Kumar[1], Dr. S.B.L. Tripathi[2], Surbie Wattal[3]

[1]Research Scholar, CMJ University, Shillong, Meghalaya (India)

[2]Ph.D. Research Guide, CMJ University, Shillong, Meghalaya (India)

[3] Research Scholar, CMJ University, Shillong, Meghalaya (India)

Abstract

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. 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.

Keywords: *Mobile Ad-Hoc Networks, MANET Protocols, Security in MANET.*

Introduction

Mobile ad hoc networks (MANETs) are dynamic collections of autonomous mobile nodes with links that are changing in an unpredictable way. They are characterized by a dynamic topology and the lack of any fixed infrastructure. The communication medium is broadcast. The nodes can be regarded as wireless mobile hosts with limited power (operating off batteries), constrained bandwidth and transmission range (typically 250–1000 meters in an open field).

The recent rise in popularity of mobile wireless devices and technological developments has made possible the deployment of such networks for several applications. Indeed, because ad hoc networks do not have any fixed infrastructure such as stations or routers, they are highly applicable for emergency deployments. These networks are decentralized, with nodes acting both as hosts and as routers, forwarding packets for nodes that are not in transmission range of each other. Several route discovery algorithms have been proposed in the literature. Theses focus mainly on efficiency issues such as scalability with respect to network size, traffic load, mobility, and on the adaptability to network conditions such as link quality and power requirements. Some of the proposed routing algorithms also address security issues but their security is restricted to rather weak adversary models. So far, most of the research has focused on functionality issues and efficiency with security being given a lower priority, and in many cases, regarded as an add-on afterthought technology rather than a design feature.

Attack Behavior

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 behavior 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).

Comparison of Passive and 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.

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.

Comparison of External and 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. 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 misbehavior activities in the ad hoc networks is not an easy task.

Comparison of Mobile and Wired Attacks

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.

Comparison of Single and Multiple Attacks

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. 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.

Modifications

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. 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. 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.

Module Description

These focus mainly on efficiency issues such as scalability with respect to network size, traffic load, mobility, and on the adaptability to network conditions such as link quality and power requirements.

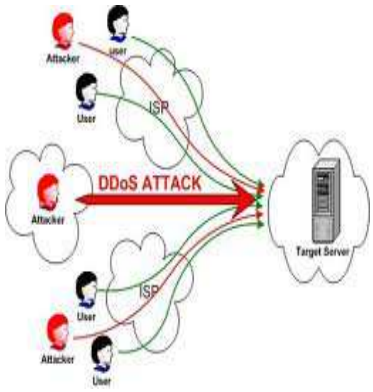

Figure1: DDos Attacks

Some of the proposed routing algorithms also address security issues for a survey, but their

security is restricted to rather weak adversary models. There are several reasons for this, the most important one being that it is hard to model a formal security framework that captures all the basic security aspects of a MANET.

SECURE ROUTE DISCOVERY

The protocol follows the RREQ/RREP procedure used by on-demand routing protocols, with several differences. To prevent outsiders from interfering, all route discovery messages are authenticated. Only authenticated nodes can initiate RREQs, and the group authenticated is required in each request. Tree nodes use the tree token to prove their tree status.

ROUTE ACTIVATION

The requester signs and unicasts on the selected route a multicast activation (MACT) message that includes its identifier, the group identifier, and the sequence number used in the RREQ phase. The MACT message also includes a one-way function applied on the tree token extracted from RREP which will be checked by the tree node that sent the RREP message to verify that the node that activated the route is the same as the initial requester. An intermediate node on the route checks if the signature on MACT is valid and if MACT contains the same sequence number as the one in the original RREQ. The node then adds to its list of tree neighbors the previous node and the next node on the route as downstream and upstream neighbors, respectively, and sends MACT along the forward route.

MULTICAST TREE MAINTENANCE

The network periodically broadcasts in the entire network a signed GroupHello message that contains the current group sequence number, the tree token authenticator, and the hop count anchor. A signed GroupHello message containing a special flag also ensures that when two disconnected trees are merging, one of the group leaders is suppressed.

DATA FORWARDING

The source periodically sends in the tree a request message that contains its data transmission rate. As this message propagates in the multicast tree, nodes may add their perceived transmission rate to it. Each tree node keeps a copy of the last heard packet. The information in the message allows nodes to detect if tree ancestors perform selective data forwarding attacks. Depending on whether their perceived rate is within acceptable limits of the rate in the message, nodes alternate between two states. The initial state of a node is disconnected; after it joins the multicast group and becomes aware of its expected receiving data rate, the node switches to the connected state. Upon detecting a selective data forwarding attack, the node switches back to the disconnected state.

Conclusion

In our work a new security framework tailored for on-demand route discovery protocols in MANETs was proposed. This represents a first effort toward a formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks the attacks that are intrinsic to the wireless broadcast medium in a neighborhood. However, as we observed above, there are a plethora of other hidden channels that become available through concurrent execution of route discovery protocols. Additionally, in the context of mobility, which requires that route discovery take place simultaneously with data communication, large additional bandwidth is naturally generated and available to adversarial nodes. Consequently, in the proposed formal model, it is impossible to prevent that adversarial nodes break up routes by inserting non existing links. To address this shortcoming, either more flexible definitions of routes must be employed (e.g., redundant routing) or it becomes necessary to address global threats directly, such as those posed by Sybil, wormhole, and more generally, man-in-the-middle attacks.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

[6] 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.