National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) 2011
Proceedings published in International Journal of Computer Applications® (IJCA)

Security Attacks in Mobile Adhoc Networks

Monu Singh[1],Ajay Singh[1],Rajesh Tanwar[1],Ritu Chauhan[2]
M.Tech Students of TIT&S Bhiwani1
M.Tech Student of MDU Campus Rohtak2

ABSTRACT
In this paper, we describe the security issues in Mobile adhoc networks. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. However, these solution are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. In this paper, the current security issues in MANET are investigated. Particularly, we have examined different routing attacks, such as flooding, black hole, spoofing, wormhole, Sybil and rerr generation attacks, as well as existing solutions to protect MANET protocols.

1. INTRODUCTION
In [1,3,4,6] Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. Such as military battle field, emergency rescue, vehicular communication, mining operation, etc. These networks are subject to frequent link breaks which also every node can perform the role of host as well as router, thus nodes which are out of transmission range can be accessed by routing through the intermediate nodes. Because of the characteristic of dynamic wireless network [9.14], MANET presents the following set of unique challenges to secure. Dynamic network: the topology of MANETs is highly dynamic as mobile nodes freely roam in network, join or leave the network on their own will, and fail occasionally. The wireless channel is also subject to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay. Mobile users roaming in the network may request for anytime, anywhere security services. Resource constraints: the wireless channel is bandwidth constrained and shared among multiple networking entities. The computation and energy resources of a mobile node are also constrained. No clear line of defense: MANET has not offer aclear line of defense. Moreover, the wireless channel is accessible to both legitimate users and malicious attackers. The boundary that separate the inside network from the outside world becomes blurred. Device with weak protection: portable devices, as well as the system security information they store, are vulnerable to compromises.

Security solutions are important issues for MANET, especially for those selecting sensitive applications, have to meet the following design goals while addressing the above challenges. Availability: ensures the survivability of the network services despite Denial of Service (DoS) attacks. A DoS attack could be launched at any layer of ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. The security service is highly available on the network layer at anytime and at anywhere. On the higher layers, an adversary could bring down high-level services. Efficiency: the solution should be efficient in terms of communication overhead, energy consumption and computationally affordable by a portable device [2].

2. RELATED WORK
A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, in [4,7] many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. Although a lot of work under progress in this subject particularly routing attacks and its existing countermeasures. The existing security solutions of wire networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. In this paper, we have discussed current routing attacks and countermeasures against MANET protocols. Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource constrained in MANET. They still not perfect in terms of tradeoffs between effectiveness and efficiency. Some solutions in [4,7,12] work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers. In addition, some may require special hardware such as a GPS or a modification to the existing protocol.

3. ROUTING ATTACKS IN MANET
The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail.

4. FLOODING ATTACK
In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service. A simple mechanism proposed to prevent the flooding attack in

the AODV protocol [15] . In this approach, each node monitors and calculates the rate of its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake. The authors show in [5] that a flooding attack can decrease throughput by 84 percent. The authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in [15] above where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

5. BLACK HOLE ATTACK

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. For example of a black hole attack, where attacker sends a fake RREP to the source node , claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node will choose the route that passes through attacker node . The route confirmation request (CREQ) is introduced in [6] and route confirmation reply (CREP) is introduced here to avoid the black hole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path. In [11] the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive. In another attempt[7] , the authors analyzed the black hole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the black hole attack, based on differences between the destination sequence numbers of the received RREPs. The key advantage of this approach is that it can detect the attack at low cost without introducing extra routing traffic, and it does not require modification of the existing protocol. However, false positives are the main drawback of this approach due to the nature of anomaly detection.

6. WORMHOLE ATTACK:-

In [8,10] a wormhole attack, a malicious node uses a path outside the network to route messages to another node at some other location in the. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. A wormhole itself does not have to be harmful; for it usually lowers the time it takes for a package to reach its destination. But even this behavior could already damage the operation, since wormholes fake a route that is shorter than the according one within the network; this can confuse routing mechanisms which rely on the knowledge about distance between nodes. Wormholes are dangerous because they can do damage without even knowing the network. The wormhole attack can be detected by marking each packet with timestamps and location stamps in order to detect wormhole intrusions in a system. Each packet is tagged with very precise time information of the sender node, which is then compared by the destination node to its own time and location stamps. If the comparison reveals an unrealistic distance the data took within an unrealistic amount of time, it can be assumed that there is a wormhole within the network .

7. SINKHOLES

In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on Adhoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate. The problem of sinkhole attack can be much amplified if the malicious node exists within or around the centre of the network so that it hears every communication happening inside the network. However, in the case of Multipath protocols which send data redundantly, not relying on one path only, the problem of sinkholes can be reduced. Probabilistic protocols which measure the trustworthiness of a network can help detecting sinkholes within the network

8. SYBIL ATTACK

Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes, this attack is called the Sybil attack. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have a harder time to destroy the integrity of information. However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded. The attacker may get access to all the data or may alter all packets in the same transmission so that the destination node/s cannot detect the change in packets anymore. In trust-based routing environments, representing multiple identities can be used to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it; in ideal starting point for further attacks.

9. SPOOFING ATTACK

In [13] spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network. This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node. A malicious node with this goal will most likely try to impersonate a node within the path of the data flow it requires. It could be done by modifying routing data or implying itself as a trustworthy communication partner to neighboring nodes in parallel. Usually, exploiting MAC layer protocol malicious nodes could place their node between two other nodes communicating with each other (man-in-the middle attack).

10. RERR GENERATION

[12]Malicious nodes can prevent communications between any two nodes by sending RERR messages to some node along the path. The RERR messages when flooded into the network, may cause the breakdown of multiple paths between various nodes of the network, hence causing a no. of link failures.

11. REFERENCES

[1] C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SlCON '97, Apr. 1997, pp. 197-211

[2] Th. Clausen et al., “Optimized Link State Routing Protocol,” IETF Internet draft, draft-ietfmanet-olsr-11.txt, July 2003.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[4] Z. Karakehayov, “Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks,” Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[5] S. Desilva, and R. V. Boppana, “Mitigating Malicious Control Packet Floods in Ad Hoc Networks,” Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[6] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks,” 2002 Int’l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[7] S. Kurosawa et al., “Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method,” Proc. Int’l. J. Network Sec., 2006.

[8] D. Johnson and D. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[9] Jyoti Raju and J.J. Garcia-Luna-Aceves, “ A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks’,” in Proceeding of IEEE ICC, June 2000.

[10] Y-C. Hu, A. Perrig, and D. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[11] M. Al-Shurman, S-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conf. 2004.

[12] M. G. Zapata and N. Asokan, “Securing Ad-Hoc Routing Protocols,” Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[13] K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 2002 IEEE Int’l. Conf. Network Protocols, Nov. 2002.

[14] C. Perkins and E Royer, “Ad Hoc On-Demand Distance Vector Routing,” 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., 1999.

[15] P. Yi et al., “A New Routing Attack in Mobile Ad Hoc Networks,” Int’l. J. Info. Tech., vol. 11, no. 2, 2005.