International Journal of Signal System Control and Engineering Application 3 (3): 34-39, 2010
ISSN: 1997-5422

A Study on Various Attacks and Attack Detection Methods in Mobile Ad-Hoc Networks

S. Kannan, T. Kalaikumaran, S. Karthik and V.P. Arunachalam
Department of Computer Science and Engineering, SNS College of Technology,
Sathy Main Road, 641035 Coimbatore, Tamil Nadu, India

Abstract: 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. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET. However, these mechanisms 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 study, the current security issues in MANET are investigated. Particularly, we have examined different routing attacks such as flooding, black hole, link spoofing attacks and some detection methods like profile-based detection, specification-based detection as well as existing solutions to protect MANET protocols.

Key words: MANET security, routing protocols, data security, shared wireless channel, countermeasure, heavy traffic

INTRODUCTION

There are 15 major issues and sub-issues involving in MANET such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia and standards/products. Currently, the routing, power management, bandwidth management, radio interface and security are hot topics in MANET research. Although in this study, we only focus on the routing protocols and security issues in MANET. The routing protocols in MANET may generally be categorized as: table-driven/proactive and source-initiated (demand-driven)/reactive. In proactive routing protocols such as the Optimized Link State Routing (OLSR), nodes obtain routes by periodic exchange of topology information. In reactive routing protocols such as the Ad-hoc on demand Distance Vector (AODV) protocol nodes find routes only when required.

The overall goal of the security solutions for MANET is to provide security services including authentication, confidentiality, integrity, anonymity and availability to the mobile users. In order to achieve to this goal, the security solution should provide complete protection spanning the entire protocol stack. We can categories MANET security in 5 layers such as application layer, transport layer, network layer, link layer and physical layer. However, we only focus on the network layer which is related to security issues to protect the ad-hoc routing and forwarding protocols. From the security design perspective, the MANETs have no clear line of defense. Unlike wired networks that have dedicated routers each mobile node in an ad-hoc network may function as a router and forward packets for other peer nodes.

The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring or access control mechanisms can be deployed. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad-hoc routing protocols such as AODV, DSR and wireless MAC protocols such as 8002.11; typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications (Al-Shurman *et al*., 2004; Ford and Fulkerson, 1962).

Recently, several research efforts introduced to counter against these malicious attacks. Most of the previous reseach has focused mainly on providing preventive schemes to protect the routing protocol in a MANET. Most of these schemes are based on key management or encryption techniques to prevent

Corresponding Author: S. Kannan, Department of Computer Science and Engineering, SNS College of Technology, Sathy Main Road, 641035 Coimbatore, Tamil Nadu, India

unauthorized nodes from joining the network. In general, the main drawback of these approaches is that they introduce a heavy traffic load to exchange and verify keys which is very expensive in terms of the bandwidth-constraint for MANET nodes with limited battery and limited computational capabilities. The MANET protocols are facing different routing attacks such as flooding, black hole, link withholding, link spoofing, replay, wormhole and colluding misrelay attack (Ford and Fulkerson, 1962; Chiang *et al*., 1997; Clausen and Jacquet, 2003).

Routing protocols in MANET: There are different criteria for designing and classifying routing protocols for wireless ad hoc networks. For example, what routing information is exchanged when and how the routing information is exchanged when and how routes are computed, etc.

Proactive vs. reactive routing: Proactive schemes determine the routes to various nodes in the network in advance, so that the route is already present whenever needed. Route discovery overheads are large in such schemes as one has to discover all the routes. Examples of such schemes are the conventional routing schemes, Destination Sequenced Distance Vector (DSDV). Reactive schemes determine the route when needed. Therefore, they have smaller route discovery overheads (Desilva and Boppana, 2005; Dow *et al*., 2005; Kannhavong *et al*., 2007).

Single path vs. multi path: There are several criteria for comparing single-path routing and multi-path routing in ad-hoc networks. First, the overhead of route discovery in multi-path routing is much more than that of single-path routing. On the other hand, the frequency of route discovery is much less in a network which uses multi-path routing since, the system can still operate even if one or a few of the multiple paths between a source and a destination fail. Second, it is commonly believed that using multi-path routing results in a higher throughput (Desilva and Boppana, 2005; Dow *et al*., 2005; Kannhavong *et al*., 2007).

Table driven vs. source initiated: In table driven routing protocols, up-to-date routing information from each node to every other node in the network is maintained on each node of the network. The changes in network topology are then propagated in the entire network by means of updates. Destination Sequenced Distance Vector Routing (DSDV) and Wireless Routing Protocol (WRP) are 2 schemes classified under the table driven routing protocols head. The routing protocols classified under source initiated on-demand routing, create routes only when desired by the source node. When a node requires a route to a certain destination, it initiates what is called as the route discovery process. Examples include DSR and AODV (Desilva and Boppana, 2005; Dow *et al*., 2005; Kannhavong *et al*., 2007).

Destination-Sequenced Distance Vector (DSDV) routing protocol: DSDV is a table driven routing protocol based on the classical Bellman-Ford routing algorithm. The improvement made to the Bellman-Ford algorithm includes freedom from loops in routing tables by using sequence numbers. In this routing protocol, each mobile node in the system maintains a routing table in which all the possible destinations and the number of hops to them in the network are recorded. A sequence number is also associated with each route/path to the destination. The route labeled with the highest sequence number is always used. This also helps in identifying the stale routes from the new ones thereby avoiding the formation of loops. Also to minimize the traffic generated, there are 2 types of packets in the system. One is known as full dump which is a packet that carries all the information about a change. However at the time of occasional movement, another type of packet called incremental will be used which will carry just the changes thereby increasing the overall efficiency of the system.

The data broadcast by each mobile node will contain the new sequence number, the destination's address, the number of hops to reach the destination and the sequence number of the information received regarding that destination. Each node advertises an increasing even sequence number for itself. When node A determines that destination node D is unreachable, it advertises the next odd sequence number for the route that has failed with an infinite metric count. Any node that receives this infinite metric count updates its table for the matching route and waits until a greater sequence number with non-infinite metric count is received. Every mobile host also calculates the weighted average of the time taken to receive a route with the best metric. This time is called the settling time (Kannhavong *et al*., 2006).

Dynamic Source Routing (DSR) protocol: DSR is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes

processing the route discovery packets. The learned paths are used to route packets (Karakehayov, 2005). This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only 2 major phases which are route discovery and route maintenance. Route reply would only be generated if the message has reached the intended destination node.

Ad-hoc on demand Distance Vector (AODV) routing protocol: AODV is capable of both unicast and multicast routing. It is a reactive routing protocol meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the internet are proactive, meaning they find routing paths independently of the usage of the paths.

AODV is as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV (Satoshi *et al*., 2006).

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.

Flooding attack: In flooding attack, attacker exhausts the network resources such as bandwidth and to consume anode'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 (Johnson and Maltz, 1996; Raju and Garcia-Luna-Aceves, 2000).

A simple mechanism proposed to prevent the flooding attack in the AODV protocol. 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. In the researchers show that a flooding attack can decrease throughput by 84%.

The researchers 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. Similar to 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 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 (Hu *et al*., 2006).

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 (IEEE 802.11, 1997).

The route confirmation request (CREQ) and route confirmation reply (CREP) is introduced in 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 2 consecutive nodes work in collusion that is when the next-hop node is a colluding attacker sending CREPs that support the incorrect path. In the researchers proposed a solution that requires a source node to wait until a RREP packet arrives from >2 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

draw back of this solution is that it introduces time delay because it must wait until multiple RREPs arrive (Lee *et al*., 2002).

In another attempt, the researchers 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 researchers 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 (Marti *et al*., 2000; Park and Corson, 1997).

Link spoofing attack: In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic for example, modifying or dropping the routing traffic or performing other types of DoS attacks (Park and Corson, 1997; Charles and Bhagwat, 1994).

A location information-based detection method is proposed to detect link spoofing attack by using cryptography with a GPS and a time stamp. This approach requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes.

This approach detects the link spoofing by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maximum transmission range. The main drawback of this approach is that it might not work in a situation where all MANET nodes are not equipped with a GPS. Furthermore, attackers can still advertise false information and make it hard for other nodes to detect the attack. In this study, researchers show that a malicious node that advertises fake links with a target's two-hop neighbors can successfully make the target choose it as the only MPR. Through simulations, the researchers show that link spoofing can have a devastating impact on the target node. Then, the researchers present a technique to detect the link spoofing attack by adding two-hop information to a HELLO message. In particular, the proposed solution requires each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the link spoofing attack is launched. The main advantage of this approach is that it can detect the link spoofing attack without using special hardware such as a GPS or requiring time synchronization. One limitation of this approach is that it might not detect link spoofing with nodes further away than three hops (Charles and Bhagwat, 1994).

ATTACK DETECTION METHODS IN MANET

Profile-based detection: Profile-based detection is also known as behavior-based detection. Profile-based detection defines a profile of normal behavior and classifies any deviation of that profile as an anomaly. The assumption of this type of detection is that attacks are events distinguishable from normal legitimate use of system resources.

Although, this type of anomaly detectors are able to detect novel attacks, they are prune to high false positive rate due to the difficulty of clear segmentation between normal and abnormal activities and the use of insufficient or inadequate features to profile normal behaviors (Potlapally *et al*., 2006; Yang *et al*., 2006; Anjum *et al*., 2005).

Specification-based detection: Specification-based detection defines a set of constraints that describe the correct operation of a program or protocol and monitors the execution of the program with respect to the defined constraints. It has been show that specification-based techniques live up to their promise of detecting known as well as unknown attacks while maintaining a very low rate of false positives. Since, the increasing popularity of wireless networks to that of wired networks, security is being considered as a major threat in them. Wireless network exposes a risk that an unauthorized user can exploit and severely compromise the network. There can be different possible attacks in wireless network viz., active and passive attacks. So, there is a need for secured wireless system to analyze and detect number of attacks (Potlapally *et al*., 2006; Yang *et al*., 2006; Anjum *et al*., 2005).

CONCLUSION

A MANET is a promising network 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, many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power,

computational power and security. Although, we have only discussed the security issues in this study, particularly routing attacks and its existing countermeasures 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 is that the solution should be efficient in terms of communication overhead, energy consumption and computationally affordable by a portable device. Authentication enables a mobile node to ensure the identity of the peer node it is communicating with. Without authentication, an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Integrity guarantees that a message being transmitted is never corrupted.

A message could be corrupted because of being failures such as radio propagation impairment or because of malicious attacks on the network. Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Non-repudiation ensures that the original message cannot deny having sent the message. No repudiation is useful for detection and isolation of compromised mobile nodes.

REFERENCES

Al-Shurman, M., S.M. Yoo and S. Park, 2004. Black hole attack in mobile Ad Hoc networks. Proceedings of the 42nd Annual Southeast Regional Conference, April 2-3, Huntsville, AL USA., pp: 96-97.

Anjum, F., S. Das, P. Gopalakrishnan, L. Kant and B. Kim, 2005. Security in an insecure WLAN network. Proceedings of the International Conference on Wireless Networks, Communications and Mobile Computing, June 13-16, USA., pp: 292-297.

Charles, E.P. and P. Bhagwat, 1994. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. Proceedings of the Conference on Communications Architectures, Protocols and Applications, Aug. 31-Sept. 2, England, UK., pp: 234-244.

Chiang, C.C., H.K. Wu, W. Liu and M. Gerla, 1997. Routing in clustered multihop, mobile wireless networks with fading channel. Proceedings of the IEEE SICON Conference, April 1997, USA., pp: 197-211.

Clausen, T. and P. Jacquet, 2003. Optimized link state routing protocol. Internet Draft, IETF Manet Working Group. http://tools.ietf.org/html/draft-ietf-manet-olsr-11.

Desilva, S. and R.V. Boppana, 2005. Mitigating malicious control packet floods in Ad Hoc networks. Proceedings of the IEEE Wireless Communications and Networking Conference, March 13-17, New Orleans, LA. USA., pp: 2112-2117.

Dow, C.R., P.J. Lin, S.C. Chen, J.H. Lin and S.F. Hwang, 2005. A study of recent research trends and experimental guidelines in mobile Ad-Hoc networks. Proceedings of the 19th International Conference on Advanced Information Networking and Applications, March 28-30, Taichung, Taiwan, pp: 72-77.

Ford, L.R. and D.L. Fulkerson, 1962. Flows in Networks. Princeton University Press, New Jersey, USA., ISBN-10: 0691079625, pp:198.

Hu, Y.C., A. Perrig and D.B. Johnson, 2006. Wormhole attacks in wireless networks. IEEE J. Selected Areas Commun., 24: 370-380.

IEEE 802.11, 1997. IEEE standard for wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Institute of Electrical and Electronics Engineers, pp: 456. http://www.techstreet.com/cgi-bin/detail?doc_no=IEEE%7C802_11_1997&product_id=36494.

Johnson, D.B. and D.A. Maltz, 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. In: Mobile Computing, Imelinsky, T. and H. Korth (Eds.). Chapter 5, Kluwer Academic Publishers, Norwell, MA, USA., ISBN: 0792396979, pp: 153-181.

Kannhavong, B., H. Nakayama and A. Jamalipour, 2006. NIS01-2: A collusion attack against olsr-based mobile Ad Hoc networks. Proceedings of the Global Telecommunications Conference, Nov. 27-Dec. 1, San Francisco, CA. USA., pp: 1-5.

Kannhavong, B., H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, 2007. A survey of routing attacks in mobile Ad Hoc networks. IEEE Wireless Commun., 14: 85-91.

Karakehayov, Z., 2005. Using REWARD to detect team black-hole attacks in wireless sensor networks. Proceedings of the Workshop on Real-World Wireless Sensor Etworks, June 20-21, Stockholm, Sweden, pp: 1-5.

Lee, S., B. Han and M. Shin, 2002. Robust routing in wireless Ad Hoc networks. Proceedings of the International Conference on Parallel Processing Workshops, Aug. 18-21, Vancouver, Canada, pp: 73-78.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile Ad Hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Aug. 6-11, Boston, Massachusetts, United States, pp: 255-265.

Park, V.D. and M.S. Corson, 1997. A highly adaptive distributed routing algorithm for mobile wireless networks. Proceedings of the IEEE 6th Annual Joint Conference on Computer and Communications Societies, April 7-12, Kobe, Japan, pp: 1405-1413.

Potlapally, N.R., S. Ravi, A. Raghunathan and N.K. Jha, 2006. A study of the energy consumption characteristics of cryptographic algorithms and security protocols. IEEE Trans. Mobile Comput., 5: 128-143.

Raju, J. and J.J. Garcia-Luna-Aceves, 2000. A comparison of on-demand and table driven routing for Ad Hoc wireless networks. Proceedings of the IEEE International Conference on Communications, June 18-22, New Orleans, LA, USA., pp: 1702-1706.

Satoshi, K., N. Hidehisa, K. Nei, J. Abbas and J. Abbas, 2006. Detecting blackhole attack on aodv-based mobile Ad Hoc networks by dynamic learning method. IEIC Tech. Rep., 105: 65-68.

Yang, H., F. Ricciato, S. Lu and L. Zhang, 2006. Securing a wireless world. Proc. IEEE, 94: 442-454.