A Survey on Routing protocols for enhancement of security of mobile ad-hoc network

Mahima Jaiswal[1] Ritesh Beohar[2]
Pg Scholar[1], Asst. Professor[2]
Electronic & Communication department
Gyan Ganga institute of Technology and Sciences

Abstract: *In this paper, a brief discussion of mobile ad hoc network, its basic requirements, its applications, security issues, and about the protocols who carry data and information's from one node to another nodes has been done. This paper enlists various protocols needed for security enhancement of mobile ad-hoc network.*

Key words: MANET, topologies, security issues, IDS, AODV.

SECTION I: Introduction

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. There are some unique characteristics of mobile ad hoc networks first, the connections between network nodes are wireless, and the communication medium is broadcast. The wireless connection provides the nodes with freedom to move, so the mobile nodes may come together as needed and form a network, not necessarily with any assistance from the cable connections. Second, unlike traditional wireless networks, mobile ad hoc networks do not have any fixed infrastructure. It is only a collection of self-organized mobile nodes, which are connected through high-variable quality links. Thus, the network topology is always changing; the execution context is extremely dynamic.

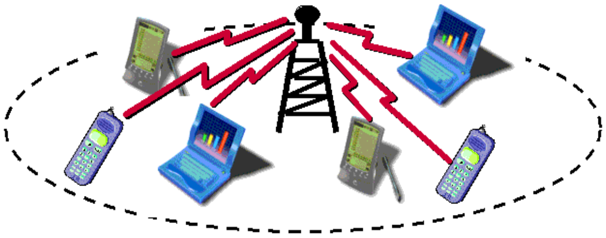

Figure 1 : MANET Structure

Section II discusses about hardware and software requirements of MANET. Section III discusses various security issues followed by conclusions in Section IV.

SECTION-II: Requirements for MANET

There are some of basic requirements for mobile ad-hoc network.

2.1 Hardware: the ad hoc networks don't have any infrastructure, except they are combined with other networks' type. Only end devices are needed to establish ad hoc. Firstly the devices must be equipped with transceiver, so they can catch the incoming signal and send a signal. Secondly the devices must be implemented after the standard IEEE 802.11. The devices like laptops, Personal Digital Assistant (PDA), smart phone are mostly implemented with the standard IEEE 802.11 so they can join an infrastructure network or ad hoc network.

2.2 Software: the most important software components of the ad hoc networks are routing algorithm. The following are some of most famous routing algorithms.

2.2.1 Destination-Sequenced Distance-Vector (DSDV): DSDV routing is a scheme for ad hoc mobile networks and an Expansion of Distance Vector Routing for ad hoc networks. DSDV is using a routing method distance vector, which is based on Distributed network. In the networks with dynamic topology this routing protocol acts very badly. This protocol has count-to-infinity problem. To gather information about the actual topology, the nodes have to swap their routing table continuously. In DSDV the routing table consists of:

(i)The destination's node address

(ii)The number of hops required to reach destination

(iii)The sequence number (or timestamp) of the information received regarding that destination, as originally stamped by the destination.

2.2.2 Dynamic Source Routing (DSR): It 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. This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply). Therefore, it is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach.

2.2.3 Ad Hoc on-Demand Distance Vector Routing (AODV): This protocol uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers. AODV is a reactive protocol, even though it still uses characteristics of a proactive protocol. AODV takes the interesting parts of DSR and DSDV in the sense that it uses the concept of route discovery and route maintenance of DSR and the concept of sequence numbers and sending of periodic hello messages from DSDV. The protocol uses different messages to discover and maintain links.

SECTION – III: Security issues of MANET

Attacks against ad hoc networks can be divided into two groups: Passive attacks typically involve only eavesdropping of data. Active attacks involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data. External attacks are typically active attacks that are targeted e.g. to cause congestion, propagate incorrect routing information, prevent services from working properly or shut down them completely. External attacks can typically be prevented by using standard security mechanisms such as firewalls, encryption and so on. Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus protected with the security mechanisms the network and its services offer. Thus such malicious insiders who may even operate in a group may use the standard security means to actually protect their attacks. These kind of malicious parties are called compromised nodes, as their actions compromise the security of the whole ad hoc network.

Denial of Service: The denial of service threat either produced by an unintentional failure or malicious action forms a severe security risk in any distributed system. The consequences of such attacks, however, depend on the area of application of the ad hoc network: In the classroom example any of the nodes, either the teacher’s centralized device or the students’ handheld gadgets, can crash or be shut down without completely destroying anything - the class can continue their work normally by using other tools. On the contrary, in the battlefield scenario the efficient operation of the soldiers may totally depend on the proper operation of the ad hoc network their devices have formed. If the enemy can shut down the network, the group may be separated into vulnerable units that cannot communicate with each other or to the headquarters.

Disclosure: Any communication must be protected from eavesdropping, whenever confidential information is exchanged. Also critical data the nodes store must be protected from unauthorized access. In ad hoc networks such information can include almost anything e.g. specific status details of a node, the location of nodes, private or secret keys, passwords and -phrases and so on. Sometimes the control data is more critical information in respect of the security than the actual exchanged data. For instance the routing directives in packet headers such as the identity or location of the nodes can sometimes be more valuable than the application-level messages. This applies especially in critical military applications. For instance in the battlefield scenario the data of a "hello" packet exchanged between nodes may not be as interesting from the viewpoint of the enemy. Instead the identities of the observed nodes - compared to the previous traffic patterns of the same nodes - or the detected radio transmissions the nodes generate may be the information just the enemy needs to launch a well-targeted attack. On the contrary, in the classroom example the disclosure of exchanged or stored information is critical "only" from the viewpoint of a person’s privacy.

SECTION IV: Conclusion

Existing ad hoc routing protocols are subject to a variety of attacks that can allow attackers to influence a victim’s selection of routes or enable denial-of-service attacks. We have shown a number of such attacks, and how they are easily exploited in ad hoc routing protocols. The best protocol can be selected for the purpose of security of MANET.

SECTION V: References

[1] S. R. Das, C. E. Perkins, E. M. Royer, and M. K. Marina, "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," IEEE personal Comm,Vol 8,pp.16-28,feb, 2001.

[2] Srdjan krco and marina dupcinov, Improved neighbour detection algorithm for aodv routing protocol, ieee communications letters, December 2003.

[3] Pradeep kumar Mani, David W Petr, Development and Performance Characterization of Enhanced AODV Routing for CBR and TCP Traffic, 864-7762 0-7803-8246-3 2004 IEEE.

[4] Zhao Qiang Zhu Hongbo, "An optimized AODV protocol in mobile ad hoc Network", In Wireless comm. networking & mobile computing 2008(WiCOM'08), 4th international conference on Oct 12-14, 2008, pp.1-4.

[5] Ammar Zahary and Aladdin Ayesh, "On-demand Multiple Route Maintenance in AODV", in Computer Engineering & System, 2008, International Conference on Nov 25-27, 2008, pp.225-230.

[6] Xinsheng Wang, Qing Liu, Nan Xu, The Energy-Saving Routing Protocol Based on AODV, Fourth International Conference on Natural Computation, 978-0-7695-3304-9/08,2008 IEEE.

[7] Mehdi Zarei, Karim Faez, Javad Moosavi Nya, Modified Reverse AODV Routing Algorithm using Route Stability in Mobile Ad Hoc Networks, 978-1-4244-2824-3,2008 IEEE.

[8] YU Bin, SUN Bin, "Modify AODV For MANET/INTERNET Connection Through Multiple Mobile Gateways", ISBN 978-89-5519-139-4 -1519- Feb. 15-18, 2009 ICACT 2009.

[9] Nastooh Taheri Javan, Reza Kiaeifar, Bahram Hakhamaneshi, Mehdi Dehghan"ZD-AOMDV: A New Routing Algorithm for Mobile Ad-Hoc Networks"2009 Eigth IEEE/ACIS International Conference on Computer and Information Science.

[10] Hothefa Sh.Jassim, Salman Yussof, Tiong Sieh Kiong, S. P. Koh1, Roslan Ismail "A Routing Protocol based on Trusted and shortest Path Selection for Mobile Ad hoc Network" Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15 -17 December 2009.