Middle-East Journal of Scientific Research 23 (5): 779-784, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.05.22202

DOS Attacks and Defenses at the Network Layer in AD-HOC and Sensor Wireless Networks, Wireless AD-HOC Sensor Networks: A Short Survey

M. Prabu, S. Vijaya Rani, R. Santhosh Kumar and P. Venkatesh

Department of CSE, Adhiyamaan College of Engineering,Hosur-635109, Tamil Nadu, India

Abstract: Adhoc and sensor wireless networks are challenging and promising field for researchers. These networkingtechnology are not only significant on science and engineering but important on a broad range of applications such as critical infrastructure protection and security, disaster relief operations, biodiversity mapping, medicine and healthcare etc. Wireless Sensor Network applications require Wireless-Adhoc Networking techniques, but both are easily susceptible to various security attacks. This paper mainly focus on DOS attacks and its defenses at the network layer proposed by different researchers in adhoc, sensor wireless networks and the vampire attacks at the routing protocol layer in the new application of wireless adhoc sensor networks.

Key words: Wireless Adhoc Network · Wireless Sensor Network · Wireless Adhoc Sensor Network

INTRODUCTION

Today's attacks are succeeding far too frequently, all due to the limitations of legacy security tools. In general attacks on data networks can be classified as either passive or active. DOS attack is considered to be active attacks which prevent the normal use or management of communication services and may take the form of either a targeted attack on a particular service, incapacitating attack.DOS attacks are frequently reported for internet connected services.DOS attacks in wireless network not only cause damage to the victim node but decrease the performance of the entire network because nodes have a limited battery power and the network can be congested due to limited bandwidth. Many forms of DOS attacks can arise which is hard to prevent. These attacks are vulnerable to all the layers of protocol stack.We now focus on DOS attacks on the network layer in adhoc networks, wireless sensor networks and its application (wireless adhoc sensor network).

Network and Routing Layer: The network layer is responsible for the delivery of individual packets from the source host to the destination host. The network layer has specific duty: Routing. Routing means determination of the partial or total path of a packet. If the number of packet increases for transmission, the network may drop or misdirect the packet.Since, adhoc and wireless sensor network does not have pre-existing infrastructure, it may add new vulnerabilities to the network layer. The design of routing protocol must be simple enough to cope with those vulnerabilities.

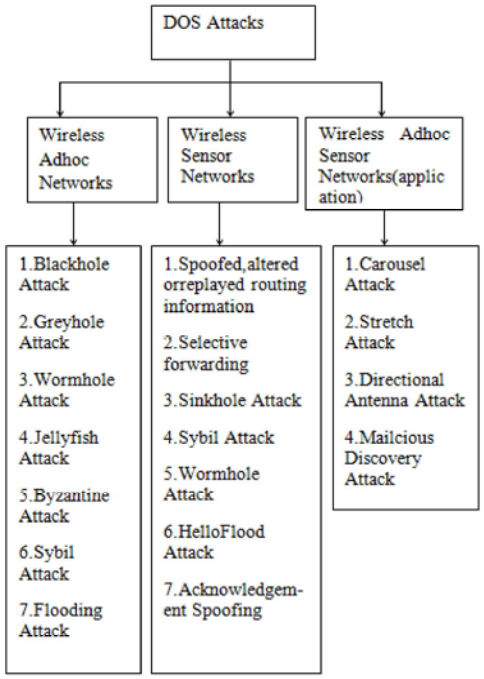

Fig. 1: Various DOS attacks at the network layer

Corresponding Author: M. Prabu, Department of CSE, Adhiyamaan College of Engineering, Hosur-635109, Tamil Nadu, India. E-mail: prabu_pdas@yahoo.co.in.

Dos Attacks and Defenses on Adhoc Network Routing

Blackhole Attack: Blackhole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network.

Yi *et al*. [1] proposed a security aware routing protocol (SAR) for wireless network which can be used to prevent blackhole attacks. It is based on on-demand protocols such as AODV or DSR. In SAR, source node adds some security metric to a RREQ(Route Request) packet and forwards it to an intermediate node followed by different route discovery procedures. An intermediate node verifies the security metric on the received RREQ packet. If the security metric is satisfied, the node will process RREQ packet and forwards to its neighbour node by using controlled flooding or else the RREQ packet is dropped. If a malicious node alters the security metric in RREQ packet in-order to intrude the flow of packets, it does not cause any serious damage since an appropriate node will drop the RREQ packet.

Greyhole Attack: Greyhole attack is similar to blackhole attack except that the malicious node will not drop all the packets, instead the selective packets are dropped. Greyhole attack is hard to detect due to partial packet loss by the malicious node and also due to congestion, overload and selfish nature.

Sukla Banerjee [2] proposed a solution for detection and removal of greyhole attack in AODV protocol. This approach is mainly used to detect the dropping of packets by the malicious node. A neighbour node monitors each node in the route. Source node sends the information with the number of packets (data count). Neighbour node checks whether it has received all the packets by verifying the data count and replies to the source via a result message.

Wormhole Attack: An intruder record packets at one location in the network and tunnels them to another location. This can be done by interrupting routing control messages.

Hu *et al*. [3] designed a packet leash protocol as a countermeasure to the wormhole attack. In this protocol, the source node adds packet life time to restrict the distance for the transmission. The receiver checks whether the packet has been reached within a time bound specified by the sender. If the constraint is satisfied, the packet is accepted otherwise it is dropped. Capkun *et al*. [4] proposed sector mechanism to detect wormholes without the necessity of clock synchronization. Hu *et al*. [5] proposed directional antennas technique to thwart wormhole attacks.

Jellyfish Attack: In jellyfish attack, the malicious node may cause the traffic without forwarding the data packets for some amount of time. This leads to high end-to-end delay and decrease the performance of a network.

Fahad Samad *et al*. [6] proposed a security scheme called JAM (Jellyfish Attacks Mitigator) to mitigate jellyfish attacks. In this scheme, MAC layer acknowledgments are sent to the source node by the destination node to indicate that it has received the sent frame successfully. When the source node does not receive a MAC acknowledgment, it has to resend the unacknowledged frame.

Byzantine Attack: An intruder has full control of an authenticated device and performs arbitrary behaviour such as creating routing loops, selectively dropping packets which results in degradation of routing services.

Baruch Awerbuch *et al*. [7] proposed a protocol called ODSBR (On Demand Secure Byzantine Routing Protocol) which is used to detect and avoid byzantine behaviour. This protocol consists of reliability metric which is based on path history. This metric is used to select the best path while routing the packets. ODSBR consist of three phases route discovery with fault tolerance, byzantine fault detection and link weight management.

Sybil Attack: A malicious user acquires multiple fake identities and pretends to be multiple, distinct nodes in the system. This malicious node can control the decisions of the system. Brian Neil Levine *et al*. [8] surveyed different approaches such as trusted certification, resource testing, trusted devices etc., to prevent sybil attack.

Flooding Attack: The attacker may send flood of packets to the destination node in order to degrade the performance of the network by creating the congestion. Nallamala Sri Hari *et al*. [9] proposed generic secure component called Flooding Attack Prevention (FAP) which can be applied to AODV routing protocol to repel the rushing attack.

Table 1: DOS attacks at the network layer in wireless ad-hoc networks

ATTACKS	DEFENSES and YEAR of PUBLICATION	AUTHORS
Blackhole Attack	Security Aware Routing Protocol (SAR) (2002)	S. Yi, P. Naldurg and R. Kravets
Greyhole Attack	AODV protocol (2008)	Sukla Banerjee
Wormhole Attack	Packet Leash Protocol (2002), Sector Mechanism (2003), Directional Antennas Technique (2004)	Y. Hu *et al*, S. Capkun *et al*, L. Hu *et al*.
Jellyfish Attack	security scheme called JAM (Jellyfish Attacks Mitigator) (2012)	Fahad Samad, Qassem Abu Ahmed, Asadullah Shaikh and Abdul Aziz
Byzantine Attack	On Demand Secure Byzantine Routing Protocol (2004)	Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita-Rotaruand Herbert Rubens
Sybil Attack	Trusted certification, Resource testing, Trusted devices (2006)	Brian Neil Levine, Clay Shields and N. Boris Margolin
Flooding Attack	Generic secure component called Flooding Attack Prevention[FAP] (2010)	Nallamala Sri Hari, N.Srinivas Rao and N.Satyanarayana

Dos Attacks and Defenses on Sensor Network Routing Spoofed, Altered or Replayed Routing Information: This is the most direct attack, where the intruder can degrade the performance of the system by spoofing, altering or replaying routing information. This enables the adversaries to create routing loops, congestion which lead to network traffic, generation of error messages, etc. Monika roopak *et al*. [10] suggests that this attack can be avoided by adding Message Authentication Code (MAC) after the message. Efficient encryption and authentication technique can be used to protect from spoofing attacks.

Selective Forwarding: In this attack, the malicious node will simply drop certain packets without forwarding to its neighbour node. The neighbour node will conclude that, it is going to seek another route for sending those packets. Karlof *et al*. [11] proposed multi-path routing which can be used to counter selective forwarding attack. Yu and Xiao in [12] proposed muti hop acknowledgments detection scheme for these types of attacks. Guorui Li *et al*. [13] proposed a sequential mesh test based selective forwarding attack detection scheme in Wireless Sensor Networks. This scheme works for cluster based sensor networks.

Sinkhole Attack: In sinkhole attack, the subverted nodes close to base advertise attractive routing information. These force nodes in the region to route data towards it which creates a 'sphere of influence'.

Ngai *et al*. [14] proposed first approach on the detection of sinkhole attacks which involves base station in the detection process. This leads to high communication cost. Prachi Bansal *et al*. [15] suggests hierarchical routing protocols which can be used to overcome sinkhole attacks. It consists of leader nodes which is responsible for forwarding information to the base station. Geographic routing protocol can also be used to prevent these types of attacks. It dynamically establishes routes to the base station by using local routing information.

Sybil Attack: An adversary node assumes identity of multiple nodes which causes ineffectiveness in a network. Sybil attack specially target for networks with fault tolerance and geographic routing protocol. James Newsome *et al*. [16] proposed several new defenses which include radio resource testing, random key pre-distribution, registration and position verification.

Wormhole Attack: In wormhole attack, two powerful adversary nodes placed in two strategic locations and advertise low cost path to the sink. All nodes in the network are attached to them looking for an optimal route. Wood *et al.* [17] proposed SeRWA (Secure Route protocol against Wormhole Attack in sensor networks).This protocol is used to detect wormhole attack without need of any special hardware. Karlof *et al*. [11] describe geographic routing protocol which is used to resist these attacks. Jen *et al*. [18] proposed modification to AODV which leads different routes to the source node but it does not guarantee that it will work against participation mode wormholes attacks.

Hello Flood Attack: In hello flood attack, new sensor node broadcasts "hello" to find its neighbour and also broadcast its route to the base station. Other nodes may choose to route data through this new node if the path is shorter. The malicious node broadcast a short path to the base station using high power transmission. Target nodes attempts to reply, but the adversary node is out of range.

Table 2: DOS attacks at the network layer in wireless sensor networks

ATTACKS	DEFENSES and YEAR of PUBLICATION	AUTHORS
	Spoofed, Altered or Replayed Routing Information Authentication technique(2014) Tushankbhardwaj, Sumitsoni	Efficient encryption and Monika roopak, andGunjanbatra
Selective Forwarding	Multi-path Routing(2003), Muti hop Acknowledgments(2006), Sequential Mesh Test based Detection Scheme(2010)	Karlof *et al*, Yu and Xiao, Guorui Li *et al*
Sinkhole Attack	Hierarchical Routing Protocol Geographic Routing Protocol(2012)	Prachi Bansal, BeenuYadav, Sonika Gill, Harsh Verma
Sybil Attack	Radio Resource Testing, Random key pre-distribution, Registration and Position verification.(2004)	James Newsome, Elaine Shi, Dawn Song and Adrian Perrig
Wormhole Attack	Secure Route Protocol against Wormhole Attack in sensor networks (2002) and Geographic Routing Protocol(2003)	Wood *et al*, Karlof *et al*
Hello Flood Attack	Identity Verification protocol(2006), Detection based on signal strength and client puzzles method (2010)	Venkata et al, Virendar Pal Singh et al
Acknowledgement Spoofing	Effective encryption and Proper authentication(2013)	Jyoti Shukla and BabliKumari

Table 3: DOS attacks at the network layer in wireless ad-hoc sensor networks (application)

ATTACKS	DEFENSES and YEAR of PUBLICATION	AUTHORS
Vampire Attacks	Modified Clean Slate Sensor Network Routing Protocol(2013)	Eugene Y.Vasserman and Nicholas Hopper
	Valuable Secure Protocol(VSP)(2014)	K.Vanitha and V.Dhivya
	Energy Weight Monitoring Algorithm(EWMA)(2013)	B. Umakanth and J. Damodhar
Carousel Attack	M-DSDV (Modified Destination Sequenced Distance Vector)(2014)	K.Abirami, R.Saranya, Dr.P.JesuJayarine
Stretch Attack	cryptographic algorithm RSA 128-bit(2014)	SamadhanManore, Chandan Singh, DhanashreeBadhan, HarshalaPatil

This attack puts the network in a state of confusion. Venkata *et al*. [19] suggests that identity verification protocol cab be used to defense against hello flood attacks. This protocol verifies the bi-directionality of a link and takes meaningful action based on message received over that link. Virendar Pal Singh *et al*. [20] proposed a solution for detection of hello flood attack which is based on signal strength and client puzzles method.

Acknowledgment Spoofing: Adversary can easily intercept messages between two parties by spoofing an acknowledgment of a message to the sender. The goal is to convince the sender that a weak link is strong, or a dead link is still active. JyotiShukla *et al*. [21] suggests that this attack can be prevented by using effective encryption and proper authentication for communication.

Dos Attacks and Defenses on Wireless Adhoc Sensor Network Routing: In precise, the integration of inexpensive, power efficient and reliable sensors in nodes of wireless ad-hoc networks enable new applications and opens new research. Ad-hoc wireless sensor networks are vulnerable to resource depletion attacks at the routing protocol layer which is called as vampire attack. The vampire attack is one of the DOS attacks which disable the network by quickly draining nodes battery power. Eugene Y.Vasserman and Micholos Hopper [22] discussed that clean slate sensor network routing protocol can be modified to resist vampire attacks during the packet forwarding phase.

K.Vanitha and V.Dhivya [23] proposed Valuable Secure Protocol(VSP) to prevent vampire attacks which consist of three phases network configuring phase, key management and communication phase. Umakanth *et al*. [24] proposed Energy Weight Monitoring Algorithm (EWMA) which is used to detect vampire attacks.

Attacks on Stateless Protocols

Carousel Attack: An adversary creates packets with the intention of introducing routing loops. It is named as carousel attack, since it sends packets in circles.

Abirami *et al*. [25] proposed M-DSDV (Modified Destination Sequenced Distance Vector) routing protocol which is based on table driven routing scheme. In this protocol, each router maintains the preferred outgoing route and an estimation of the time or distance to reach target node. This protocol avoids the routing loop problem. SamadhanManore *et al*. [26] proposed an algorithm to prevent from carousel attack. This algorithm involves two function forward_packets and verify_packets. The verify_packets function discards the duplicate packets which arrive at the same node.

Stretch Attack: An adversary constructs artificially long routes, possibly traversing every node in the network with the intention of draining the battery power of the sensor nodes. SamadhanManore *et al*. proposed the technique which uses cryptographic algorithm RSA 128-bit to prevent from stretch attacks.

Attacks on Stateful Protocols

Directional Antenna Attack: In this attack the vampires waste energy by restarting a packet in various parts of network and it have little control over the packets progress.

Malicious Discovery Attack: This attack falsely claims that a link isdown or claims a new link to non- existent node. It is also called as spurious route discovery.

CONCLUSION

Thus the various DOS attacks and its defenses at the network layer in wireless ad-hoc networks, wireless sensor networks and wireless ad-hoc sensor networks (application) have been discussed. This survey may help to know about various existing scheme for detection or prevention of DOS attacks at the network layer. Most security threats to wireless ad-hoc networks are applicable to wireless sensor networks. Some of these threats can be countered by encryption, data integrity and authentication.

REFERENCES

1. Yi S., P. Naldurg and R. Kravets, 2002. Security-Aware Ad-hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC.
2. Banerjee Sukla, 2008. Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks. Proceedings of the World Congress on Engineering and Computer Science 2008WCECS 2008, San Francisco, USA.
3. Hu Y., A. Perrig and D. Johnson, 2002. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. Proc. of IEEE INFORCOM.
4. Capkun, S., L. Buttyan and J. Hubaux, Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.
5. Hu L. and D. Evans, 2004. Using Directional Antennas to Prevent Wormhole Attacks.Proc. of Networks and Distributed System Security Symposium (NDSS).
6. Fahad Samad, Qassem Abu Ahmed, AsadullahShaikh and Abdul Aziz, 2012. JAM: Mitigating Jellyfish Attacks in Wireless Ad Hoc Networks. Communications in Computer and Information Science, 281: 432-444.
7. Awerbuch Baruch, Reza Curtmola, David Holmer, Cristina Nita-Rotaru and Herbert Rubens, 2004. Mitigating Byzantine Attacks in Ad HocWireless Networks. Technical Report Version.
8. Brian Neil Levine, Clay Shields and N. Boris Margolin, 2006. A Survey of Solutions to the Sybil Attack. Technical report.
9. Sri Hari Nallamala, N. Srinivas Rao and N. Satyanarayana, 2010. A Novel Routing Attack in Mobile Ad Hoc Networks. Indian Journal of Computer Science and Engineering, 1(4): 382-391.
10. roopak Monika, Tushankbhardwaj, Sumitsoni and Gunjanbatra, 2014. Review of Threats in Wireless Sensor Networks. International Journal of Computer Science and Information Technologies, 5(1): 25-31.
11. Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: attacks and countermeasures in Ad Hoc Networks, 1(2): 293-315.
12. Yu, B. and B. Xiao, 2006. Detecting selective forwarding attacks in wireless sensor networks. Proc. of the 2nd International Workshop on Security in Systems and Networks, pp: 1-8.
13. Li Guorui, Xiangdong Liu and Cuirong Wang, 2010. A Sequential Mesh Test based Selective Forwarding Attack Detection Schemein Wireless Sensor Networks, pp: 554-558.

14. Ngai, E.C.H., J. Liu and M.R. Lyu, 2006. On the intruder detection for sinkhole attack in wireless sensor networks. Proceedings of the IEEE International Conference on Communications (ICC '06), Istanbul, Turkey.
15. Bansal Prachi, BeenuYadav, Sonika Gill and Harsh Verma, 2012. Security Attacks in Wireless Sensor Network, International Journal of Scientific and Engineering Research, 3: 4.
16. Newsome James, Elaine Shi, Dawn Song and Adrian Perrig, 2004. The Sybil Attack in Sensor Networks:Analysis and Defenses.IPSN'04, Berkeley, California, USA.
17. Wood, A. and J. Stankovic, 2002. Denial of service in sensor networks. In Computer, 35: 54-62.
18. Venkata, C. Giruka, MukeshSinghal, James Royalty and Srilekha Varanasi, 2006. Security in wireless networks. Wiley Inter Science.
19. Pal Singh Virendra, Sweta Jain and JyotiSinghai, 2010. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. International Journal of Computer Science Issues, 7(3): 11.
20. JyotiShukla and BabliKumari, 2013. Security Threats and Defense Approaches inWireless Sensor Networks: An Overview, International Journal of Application or Innovation in Engineering and Management, 2: 3.
21. Eugene, Y. Vasserman and Nicholas Hopper, 2013. Vampire attack Draining life from wireless ad-hoc sensor networks. IEEE Transactions on Mobile Computing, 12: 2.
22. Vanitha, K. and V. Dhivya, 2014. A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks. IEEE International Conference on Innovations in Engineering and Technology.
23. Umakanth B. and J. Damodhar, 2013. Detection of Energy draining attack using EWMA inWireless Ad Hoc Sensor Networks. International Journal of Engineering Trends and Technology (IJETT), 4(8).
24. Abirami K., R.Saranya and Dr.P.JesuJayarine, 2014. Maintaining Lifetime of Wireless Ad-hoc Sensor Networks by Mitigating Resource Depletion Attack using M-DSDV, International Journal for Research and Development in Engineering.
25. ManoreSamadhan, Chandan Singh, DhanashreeBadhan and HarshalaPatil, 2014. Prevention of Battery Violation in WSN using Routing Loop.International Journal of Emerging Technology and Advanced Engineering, 4(2).