Journal of Information & Communication Technology
Vol. 4, No. 2, (Fall 2010) 01-10

Denial of Service Attacks in Wireless Ad hoc Networks

Safdar Ali Soomro*
Faculty of Science and Technology, Yala Islamic University, Thailand

Sajjad Ahmed Soomro*
Department of Computer Science and Engineering, Yanbu University College, Saudi Arabia

Abdul Ghafoor Memon*
Institute of Mathematics & Computer Science, University of Sindh, Pakistan

Abdul Baqi*
Computer Engineering Department, Salaman Bin Abdul Azizi University, Saudi Arabia

ABSTRACT

During the past decade, the speed and reliability of communication over wireless network has been increased drastically. One area of great interest in distributed system is wireless ad-hoc network (WANETs) that allows collaboration in real time. Wireless ad hoc networks are formed by a set of hosts that communicate with each other over a wireless channel. Denials of Service attacks are real threat to wireless systems such as WANETs. This paper provides a survey of these attacks in WANETs.

Keywords : Wireless Ad hoc Networks, Security and Privacy, Denial of Service

1. INTRODUCTION

A wireless ad hoc network (WANET) is a collection of self configuring autonomous mobile radio nodes that communicate with each other over a wireless channel. The nodes cooperate with each other in order to manage the network such as medium access control, routing each others' packets, election of a coordinator.

In recent years, MANETs have become more popular due to low prices and their ability to be deployed under normal and harsh conditions while supporting high data rates. They can be easily deployed in situations where no infrastructure exists and where it would be impractical to deploy infrastructure such as in rescue operations or seminars.

* The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (Biztek) or Yala Islamic University, Thailand, Yanbu University College, Saudi Arabia, University of Sindh, Pakistan & Salaman Bin Abdul Azizi University, Saudi Arabia

* Safdar Ali Soomro : safdarali@yiu.ac.th
* Sajjad Ahmed Soomro : Sajjad.soomro@yuc.edu.sa
* Abdul Ghafoor Memon : ghafoor@usindh.edu.pk
* Abdul Baqi : abaqi@hotmail.com

Due to the absence of a central trusted router in WANETs, nodes have to trust each other when routing data packets. The required mutual trust makes WANETs vulnerable to misbehaviors that may arise for several reasons:

1. Faulty nodes may misbehave due to configuration errors or some hardware errors.
2. Selfish nodes may not cooperate in network protocols in order to save energy.
3. Malicious nodes mount attacks with the intent of damaging the network or extracting valuable information from the network.

Regardless of misbehavior type, it may cause a performance degradation of the whole network. Therefore, there is a need to secure network protocols in WANETs.

A Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.

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. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.

Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message. No repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

In this paper we focus on DOS attacks in wireless ad hoc networks. An attacker causes congestion in the network by either generating an excessive amount of traffic by itself, or by having other nodes generate excessive amounts of traffic. In wireless networks, DOS attacks are difficult to prevent and protect against. They can cause a severe degradation of network performance in terms of the achieved throughput and latency.

2. TYPE OF ATTACKS

In general, two kinds of attacks are launched against wireless networks, passive and active attacks. Passive attacks achieve their goals without disrupting the operation of the communication. They include eavesdropping on packet exchange within the wireless

channel to achieve different goals such as launching offline attacks to find out a secret key, e.g. [2, 3] exploit a well known vulnerability in IEEE 802.11 MAC protocol that uses wired equivalent privacy (WEP) algorithm for data encryption. The attacker needs only to capture a certain amount of encrypted packets in order to launch a probabilistic attack to find out the encryption key within some seconds. An attacker can also know more about the network topology by analyzing routing packets. For example, when a specific node is requested more frequently, then the attacker may anticipate that this node plays an important role in the network and may launch a denial of service (DoS) attack on it. Jellyfish attacks are also passive attacks, as they conform to all protocol specifications and do not inject any packet in the network. Detecting passive attacks is a hard task. In active attacks, Goals are achieved by disrupting the normal functionality of the communications. Active attacks include modification of packets, creation of false packets and continuous channel access.

3. DENIAL OF SERVICE ATTACKS

A Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of his/her network connection. Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' access to a service provider.

They have numerous forms and they are hard to prevent. For instance, an attacker may send an excessive amount of requests to a server that has to test their legitimacy. This test requires an amount of CPU and memory capacity. Due to the excessive number of requests, the server will be busy in testing illegal request and will be unavailable for legal users. In comparison with wired networks, DoS attacks in MANETs may not only bring damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be congested due to the limited bandwidth available as compared to fixed networks.

Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' access to a service provider. They have numerous forms and they are hard to prevent. For instance, an attacker may send an excessive amount of requests to a server that has to test their legitimacy. This test requires an amount of CPU and memory capacity. Due to the excessive number of requests, the server will be busy in testing illegal request and will be unavailable for legal users. In comparison with wired networks, DoS attacks in MANETs may not only bring damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be congested due to the limited bandwidth available as compared to fixed networks.

Physical Layer: DoS attack can be launched against physical layer by using radio jamming device or by source of strong noise to interfere the physical channels and may compromise the service availability. For jamming attack in WMN, the attacker can launch the attack from anywhere. Due to the vast coverage area and dense deployment of wireless mesh routers in WMN, it is more vulnerable to physical layer DoS attacks. Different types of jamming attacks [5] are:

1) Trivial Jamming Attack: In which an attacker constantly transmits noise. 2) Periodic Jamming Attack: In which an attacker transmits a short signal periodically. These transmissions can be scheduled often enough to disrupt all other communications, for example, with a period less than the AIFS. It is also called scrambling. 3) Reactive Jamming Attack: In which an attacker transmits a signal whenever it detects that another node has initiated a transmission, causing a collision during the second portion of the message.

MAC Layer

MAC layer incorporates functionality uniquely designed to WMN as stated in draft 3.0 released in March, 2009 [4]. In particular, this includes the ability to discover networks, join and leave networks, and coordinate access to the radio medium. Possible DoS attacks are given below [6]:

1) MAC Misbehavior: DoS attack can be implemented via corrupting CTS / RTS frames by following steps:

a) Unprompted CTS Attack: An attacker transmits a CTS message with a long message duration causing all recipients to halt transmission for this duration.

*b) Reactive RTS Jamming Attack***:** Whenever a node detects an RTS message, it disrupts these messages by immediately initiating a transmission. The effects of this attack are exacerbated by the exponential back-off scheme.

c) CTS Corrupt Jamming: Upon receipt of a RTS message, an attacker transmits noise during the CTS response.

2) Selfish attack: The selfish nodes will reduce the resource of Wireless channel which can be used by legitimate nodes, thereby affect the network performance, and even interrupt the network service. There are two categories of selfish nodes in WMN, selfish client nodes and selfish router nodes. Selfish client nodes access WMN with selfish strategy to achieve greater throughput, reduce power consumption and improve QoS. Selfish router nodes use selfish strategy top result in the congestion of network or even the denial of service. With the

characteristics of multi-hop and public access, it is more vulnerable for WMN to selfish client nodes attack. The selfish attacks in router nodes will also have significantly impact on the entire network performance.

Routing Layer

According to Draft 3.0 released in March, 2009 [3], RA-OLSR routing protocol has been eliminated and HWMP exists. Various DoS attacks are listed below [7].

1) Blackhole Attack: In this attack, the malicious nodes broadcast itself as most optimal node for data forwarding. The malicious nodes then drop packets and hence deny the service.

2) Greyhole attack: This attack is a small variation from the Blackhole attack. In opposition to the Blackhole attack, Greyhole routers (malicious nodes) do not drop all the packets just drop selective packets.

3) Wormhole attack: In a wormhole attack, an attacker receives packets at one point in the network, "tunnels"them to another point in the network in order to create a shortcut (or wormhole) [8] in the network through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker, and then replays them into the network from that point. The malicious node can use this position to maliciously drop packets in order to deny the services in the WMN.

4) Jellyfish attack: It is done by complying protocols for packet dropping in malicious way to deny the services.

5) Byzantine attack: Attacks where the adversary has full control of an authenticated device and can perform arbitrary behavior to disrupt the system are referred to as Byzantine

attacks [9].

6) Sybil attack: A Sybil attack [10] is essentially an impersonation attack, in which a malicious device illegitimately fabricates multiple identities, behaving as if it were a larger number of nodes (instead of just one). Malicious device additional identities are referred to as Sybil identities or Sybil nodes.

7) Flooding attack: The attacker transmits a flood of packets toward a target node or to congest the network and degrade its performance. A flooding DOS attacks are difficult to handle. Attacker may use any type of packets to congest the network.

4. COUNTERMEASURES FOR DOS ATTACKS

There are several countermeasures possible [28]. These are discussed step-by-step here.

4.1 Firewall and router filtering

Firewalls are already being used to monitor packet traffic, and protect systems from malicious access. As a countermeasure to DOS attacks, Schuba et al. mentions that firewalls can be configured as a relay, or as a semi-transparent gateway [11]. Ferguson, Senie, and the SANS institute have outlined specific steps to configure and use firewalls and routers as DOS countermeasures..

4.1.1 Firewall as semi-transparent Gateway:

In this approach, the firewall passes SYN packets to the host. When the host responds with a SYN+ACK packet, the firewall forwards this packet to the client, and sends an ACK (pre-acknowledgement) packet to the host. If the firewall does not receive a legitimate ACK from the client after some timeout period, an RST packet is sent to the host to terminate the connection. For legitimate connections, the duplicate ACK arriving at the host is discarded by the TCP protocol, and future packets flow without intervention by the firewall.

Strengths: No delays introduced for legitimate connections.

Weaknesses: Timeout period needs to be carefully selected so access is not denied to legitimate connections with long response times.

4.1.2 Firewall as a Relay:

In this approach, the firewall responds on behalf of the internal host. A connection to the host is established only after the three-way handshake is successfully completed. During an attack, the firewall responds to the SYN sent by the attacker; since the ACK never arrives, the firewall terminates the connection with an RST packet, and the host never receives the datagram. For legitimate connections, the firewall creates a new connection to the internal host on behalf of the client, and continues to act as a proxy for translating sequence numbers of packets flowing between the client and server [11].

Strengths: Host is completely shielded from DOS attacks, and never receives spoofed SYN packets.

Weaknesses: New delays are introduced for legitimate connections.

4.1.3 Ingress filtering:

An attacker may forge the source address from which it is launching a DOS attack. The attacker forging its source address will cause the victim to send a SYNACK packet to an

erroneous address, preventing the victim from ever receiving the ACK packet it needs to proceed.

In RFC 2267, Ferguson and Senie described network ingress filtering that can prevent attackers from using forged source addresses to launch a DOS attack [12].

Strengths: Effectively stops attackers within the originating network from forging source addresses that do not conform to ingress filtering rules.

Weaknesses: This technique does nothing to address flooding attacks that originate from valid IP addresses, and may negatively affect mobile IP services [12].

4.1.4 Egress filtering:

SANS institute urged network administrators to adopt egress filtering, which prevents one's network from being the source of forged communications used in DOS attacks [13]. This ensures that only IP packets with valid source IP addresses leave the network.

Strengths: Useful when deployed close to the end user. Effectively deters attackers from victimizing others with one's network resource.

Weaknesses: Egress filtering becomes difficult for Internet Service Providers and almost impossible for major service providers. These service providers frequently need to forward legitimate traffic that is not part of its own address space [13].

4.1.5 Disable broadcast amplification:

A network can act as an amplification site to flood other networks with DOS attacks such as the "smurf" or "fraggle" attack. Senie urged administrators to block the receipt and forwarding of network-prefix-directed broadcast on routers through RFC 2644 [14].

Strengths: Combined with egress filtering, this technique will prevent participation in a "smurf" or "fraggle" attack.

Weakness: Broadcast amplification is a useful diagnostic tool. Without a broadcast amplifier, the WINS server on the network will not receive the broadcast, causing some name resolution on Windows systems to fail [15].

4.2 Operating system improvements

4.2.1 Brute force

Solaris/SUN has considered implementing several OS revisions to handle DOS attacks. In 1996, an information bulletin announced that SUN considered using priority queues to grant requests originating from addresses that have given successful handshakes in the past [16].

This bulletin gave an example of improvements achieved for a server with 25 listening ports, and an 8,192-entry queue, by merely upgrading its memory from 64MB to 128MB. At 600 bytes/entry, the system coped well under an all out SYN flood attack because the total memory consumed would be 120MB [16].

Strengths: These brute force improvements require large amounts of protected kernel memory. They are relatively easy to implement, and successful attacks are less likely because attackers would need to flood connection requests at a rate exceeding reasonable bandwidth capabilities.

Weaknesses: Server response time may be slower due to the larger "connection pending" data structure it needs to search [17].

4.2.2 Request Dropping

SUN considered request dropping as a control mechanism to handle SYN flooding attacks (see section 2.2.1). Alan Cox proposed a change to Linux TCP for protection against SYN flood DOS attacks by using random drop [18].

This admission control mechanism drops a pending request from a full connection request queue. The algorithm can pick a request at random, select the oldest request, or use a combination of both, to deal with a queue under attack [16]. Ricciulli, Lincoln, and Kakkar revised an analytical model for the random drop algorithm, and used a high-fidelity simulation to compare random request dropping with three other cookie-based SYN flooding defense mechanisms.

Strengths: Ricciulli et al. reported that random dropping worked well in both low congestion and high congestion by keeping client performance losses below 10%, even under very high spoofed SYN rates [17].

Weaknesses: An attacker can occasionally deny a legitimate connection request.

4.2.3 Security Architecture

Spatscheck and Peterson described a three step process called the Escort security architecture, to protecting the Scout operating system against DOS attacks: 1) Accounting for resources consumed by every principal; 2) Detection of an DOS attack when a principal's consumption of resources exceeds levels allowed by the system policy; 3) Containment of an attack to reclaim consumed resources with as few additional resources as possible [19].

Strengths: The Escort architecture supports end-to-end resource accounting, and multiple hardware-enforced protection domains so un-trusted modules can be isolated from each other. It can successfully detect and remove offending clients while delivering quality-of-service guarantees to other clients with very low overhead.

Weaknesses: The Escort architecture appears to work only on the Scout operating system, and has yet to be extended to popular operating systems such as Unix, Linux, and Windows.
4.3 Protocol improvements

Because TCP SYN flood attacks exploit an inherent weakness of the protocol, it seems reasonable to make the protocol resistant to these attacks.

4.3.1 Cookies

Cookie-based approaches change in the TCP signaling behavior by using one-way hash functions to verify the authenticity of connection requests.

Bernstein and Bona suggested a stateless cookie approach. When a client sends a SYN packet, the server calculates a one-way hash of the sender's sequence number, ports, the server's secret key, and a counter that changes every minute. The server sends the result of the one-way hash to the client, and the connection is not established. When the client replies with an ACK packet, the server recalculates the same hash function and throws away the packet if it fails to authenticate with the server. Otherwise, set up the Transmission Control Block, if it doesn't already exist [20, 21].

Strengths: Memory is never exhausted by SYN flood DOS attacks, as CPU time is used to calculate hash values.

Weaknesses: In case of packet loss, the server is prevented from sending SYN+ACK packets, breaking TCP semantics [17]

4.3.2 Stateless protocols

Aura and Nikander described weaknesses of stateful protocols, and methods to change stateful protocols into stateless ones. Stateful protocols have an upper limit on number of simultaneous connections, because there is a limited space available for storing connection state information. When this limited space is exhausted, new connections are refused. To remedy this, the state information is stored on the client rather than on the server [22]. To ensure integrity and confidentiality of state data and connection, the data stored on a client can be encrypted with the server's key.

Strengths: Optimizes the server's behavior under stressful conditions. Weakness: May be vulnerable to re-play attacks. New protocols approaches require changes to existing protocols.

4.3.3 Client-Puzzle protocols

To prevent junk mail, Dwork and Naor proposed requiring a sender to compute a moderately hard pricing function or cryptographic puzzle for each message; the cost to compute the pricing function is negligible for normal users, but high for mass mailers [23]. Juels and Brainard extended the idea so that if a server suspects it is under a DOS attack, small cryptographic puzzles are sent to clients making requests. To complete its requests, a client must solve its puzzle correctly [24].

Strengths: Cryptographic puzzles can have varying levels of difficulty (different sizes), so that the difficulty can increase as an attack becomes more severe. Weakness: Requires client-side software capable of solving the puzzle.

4.3.4 Theoretical work

Meadows proposed a formal framework and evaluation method for thinking about DOS attacks, and showed how existing tools such as the NRL Protocol Analyzer can be modified to use the proposed framework [25].

The paper contains a sample application of the theoretical framework to the Station-to-station protocol proposed by Diffie, van Oorschot, and Wiener; the author found several DOS vulnerabilities in the protocol. Because it is difficult to prove the correctness of a protocol, automated protocol analysis tools can help reveal vulnerabilities.

4.4 Intrusion Detection

Intrusion Detection (ID) systems are relatively new tools that use engines and agents to spot and analyze anomalies in the network, and alert administrators of network attacks. An ID system is a dynamic monitoring complement to the static monitoring abilities of the firewall. ID systems work by listening to all packets on a network in promiscuous mode, very much like a network sniffer does. Network packets are next analyzed for rule violations by a pattern recognition algorithm. When rule violation(s) are detected, the ID system may alert the administrator, and some can even launch retaliatory attacks. ID products available include RealSecure by Internet Security Systems, IntrusionAlert by Unified Access Communications, SecureNet Pro by Intrusion.com, NetProwler by Axent, and freeware such as Snort.

Strengths: Reybok and Engle's article on securityfocus.org suggests that ISS RealSecure is an excellent tool for detecting intrusions [26]. ID systems are designed to detect violations

to usage policies, virus activity, and pre-attack probes, and other malicious hacking activities. Thus, ID capabilities transcend DOS detection.

Weaknesses: In 1998, Ptacek and Newsham described ways to evade ID systems using insertion attacks, evasion attacks, and DOS attacks. The authors of the paper found serious weaknesses in four 1996 versions of popular products (RealSecure, NetRanger, SessionWall, and Network Flight Recorder). Insertion and evasion attacks disrupt reassembly of packets, causing ID systems to accept packets that hosts should reject. They also claimed that the "fail-open" nature of ID systems doesn't deny a hacker's access to the victim network when a monitor system becomes unresponsive due to a DOS attack. For ID systems that are capable of retaliatory attacks, the ID system may be tricked into retaliating a host that has not perpetrated any attacks [27]. Many of these vulnerabilities have been addressed in recent versions of ID systems.

Many ID systems rely on rule-based algorithms and these rules need to be updated as new attacks are discovered. ID systems need to be maintained to keep these rules up to date. In April 2000, Securityfocus.org reported that RealSecure uses a Microsoft Jet database to store data collected from detectors at the console. The size of this MDB file cannot exceed 1 Gigabyte, and must be frequently purged [26].

REFERENCES

[1] http://embassyinvestigations.org/2011/06/05/securing-ad-hoc-networks/
[2] Andrea Bittau, Wi-Fi Exposed, Crossroad-The ACM Student Magazine, Vol. 11, no.1, September 2004.
[3] Mohammed, L.A., Issac B., "DoS Attacks and Defense Mechanisms in Wireless Networks", In 2nd International Conference on Mobile Technology, Applications and Systems, 2005
[4] IEEE 802.11s Draft 3.0 released in March, 2009.
[5] Jeremy J. Blum, Andrew Neiswender and Azim Eskandarian,"Denial of Service Attacks on Inter-Vehicle Communication Networks" in 11th IEEE conference on Intelligent Transportation Systems, 2008, pp 797-802.
[6] John Bellardo and Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" in Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12, pp 2-2.
[7] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, "Denial of Service Resilience in Ad Hoc Networks" in Proceedings of the 10th annual international conference on Mobile computing and networking ,2004, pp 202-215.
[8] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Wormhole Attacks in Wireless Networks" in IEEE Journal on Selected Areas in Communications. 24(2), February 2006, pp 370-380.
[9] Kai Han1, Binoy Ravindran1, and E. Douglas Jensen, "Byzantine-Tolerant, Point To-Point Information Propagation in Untrustworthy and Unreliable Networks" in International Conference on Network-Based Information Systems, 2007.
[10] Douceur, J.R., Donath, J.S. "The sybil attack". In: Proceedings for the 1st International Workshop on Peer-to-Peer Systems, 2002, pp 251-260.
[11] C. Schuba, I. Krsul, M. Kuhn, E. Spafford, A. Sundaram, D. Zamboni, "Analysis of a Denial of Service Attack on TCP", Proceedings of the 1997 IEEE Symposium on Security and Privacy.
[12] P. Ferguson, D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" RFC 2267, January 1998.
[13] "Egress Filtering v 0.2" GIAC Special Notice, SANS Institute Resources, February 2000.
[14] D. Senie, "Changing the Default for Directed Broadcasts in Routers", RFC 2644, August 1999.
[15] CIAC, "K-032: DDoS Mediation Action List", Information Bulletin, April 2000.

[16] CIAC, "H-02: SUN's TCP SYN Flooding Solutions", Information Bulletin, October 1996.
[17] L Ricciulli, P. Lincoln, P. Kakkar, "TCP SYN Flooding Defense", CNDS 1999.
[18] A. Cox, "Linux TCP Changes for protection against the SYN attack", September 1996.
[19] O. Spatscheck, L. Peterson, "Defending Against Denial of Service Attacks in Scout"
[20] D. J. Bernstein, "Syn floods - a solution"
[21] R. Bona, "TCP SYN attacks - a simple solution"
[22] T. Aura, P. Nikander, ICICS '97, Lecture Notes in Computer Science 1334, November 1997, P. 87-97, Springer 1997
[23] C. Dwork, M. Naor, "Pricing via Processing or Combating Junk Mail"
[24] A. Juel, J. Brainard, "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks", NDSS '99, Proceedings of the 1999 Network and Distributed System Security Symposium
[25] C. Meadows, "A Formal Framework and Evaluation Method for Network Denial of Service"
[26] "Deploying ISS Realsecure in a Large Scale Environment"
[27] T. Ptacek, T. Newsham, "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection"
[28] http://faculty.lasierra.edu/~dlin/classes/cpsc433/cpsc433.htm
[29] http://www.cert.org/tech_tips/denial_of_service.html
[30] http://www.denialinfo.com/dos.html