DDoS Mitigation: An Approach Based on Network Intrusion Detection System

[1]Deepak Kumar, [2]Latha Banda

[1]PG Scholar, [2]Associate Professor
[1]Department of Computer Science & Engineering,
[1]Lingaya's Vidyapeeth, Faridabad, Inia

Abstract: DDoS attack is a threat to cyber security, its purpose is to disrupt the network or server's normal operation. DDoS attacks can disable large enterprises from providing internet services. The objective of DDoS attacks is usually to flood the target network device or even the network itself with huge number of packets. DDoS attack operates by utilizing a large network of remote computers called botnets, grouped together in order to overwhelm another system's connection or processor causing it to deny services to the legitimate traffic. The attack is relatively easy to perform but are hard to defend. Recognition of malicious packets is a complex task due to the similarity between legitimate and malicious packets, proposed DDoS mitigation technique is based on the Intrusion Detection and Prevention System along with diversion through routing and filtering for weeding out the malicious traffic. This paper gives an approach to mitigate the DDoS attacks using NIDS with Multilayer of firewall.

***Keywords* - DDoS, Botnets, Types of DDoS attacks, IDS, IPS, HIDS, NIDS.**

I. Introduction

Goal of distributed denial of service (DDoS) attack is to create malicious traffic on a target network in order to restrict access to a network resource or internet service. DDoS attacks are not very complex in nature, it makes use of the common architectural flaw in the network security. It attacks does not require a great skill to carry out Denial of Service or Distributed Denial of Service attacks. DDoS attackers may not be hacker at all as they uses the scripts available on the internet to cause a denial of service attacks. Anyone can use these scripts as its source codes are available on github and other repositories. An organization may use these scripts to test their network security and by simulating such types of attack they ensure that security measures are good enough to mitigate these attacks. In order to achieve their goal now the most common tools that are known throughout history for performing a Doss attack are low orbit ion cannon, high orbit ion cannon and slowloris which are tools that are designed to generate fake packet requests and massively spam a port on another computer with it until you overwhelm or saturate their connection it's also capable of sending packets that require a reply like a ping or something to that effect computer is forced to saturate both its downstream and its upstream and respond to a target that's not where the packet truly originated from this is called spoofing. Denial of Service attacks can take multiple computers on the internet and target them all.

These attacks are effective because of the massive volume of people that are attacking those servers and the diversity of where those attacks are coming from because host computers or bots are on the public network or internet so it is not possible to block the origin of traffic as blocking all traffic from one IP range would effectively take your network offline.

A bot network is deployed, the logical way to do this is by infecting multiple computers with a back door that allows to remotely execute or channel traffic through that device without user knowing that it's even happening now since most computer users are not about network throughput and security. They believe that the internet is slowing down when realistically what's happening on their computers that's participating in a huge coordinated effort to attack a single target somewhere on the internet.
We used DDoS attack tools (LOIC, HOIC, SLOWLORIS) for simulating attack. The technique used for DDoS Mitigation is IDS/IPS Service offered by Clear OS in combination with Snort and IDS Signature. Snort[1] is an intrusion prevention system (IPS) developed and distributed by Cisco. It is an open source package that is capable of monitoring real-time traffic and packet logging. Snort has ability to analyse protocol and ports, content matching and searching of content, and detection of numerous attacks. It offers packet sniffing similar to tcpdump and can also function as a packet logger or a complete NIDS.

II. Botnets

Botnet as the name suggests is a network of malware. Botnets gets installed on computer system through Trojan horse. General user might not be aware of the existence of botnet or malware in the system which makes it more dangerous. Malware works in the background without affecting the ongoing operations of system but it fetches sensitive information and forwards it to botmaster, A botmaster can use this information for his own financial benefits. Botmaster or the owner of bot network can command them for remotely executing a task. An attacker uses botnets for disrupting services on internet. They command the botnets to overload a network, network device or websites. Overloading slows down the network reachability to an extent that it stops functioning at all and any request to access is denied, is called a denial of service attack. The most common ways that gets a bot installed on your computers by going to malicious websites and clicking on misleading links that allows to install a payload on computer. Unfortunately, most malware and virus detectors cannot find many of these backdoors because these backdoors that are being installed they're doing it in a way that makes it look like activity that a normal application would do and because it doesn't have that signature of a virus the detector has no way of knowing that it's malicious. It relies on Internet traffic and thus the spyware detector malware detector has no idea what traffic is actually going through it until somebody discovers the bot and actually reports it. Realistically the only safe way to protect yourself from having a bot installed on your computer is to not visit malicious websites make sure you only visit websites that are secure.

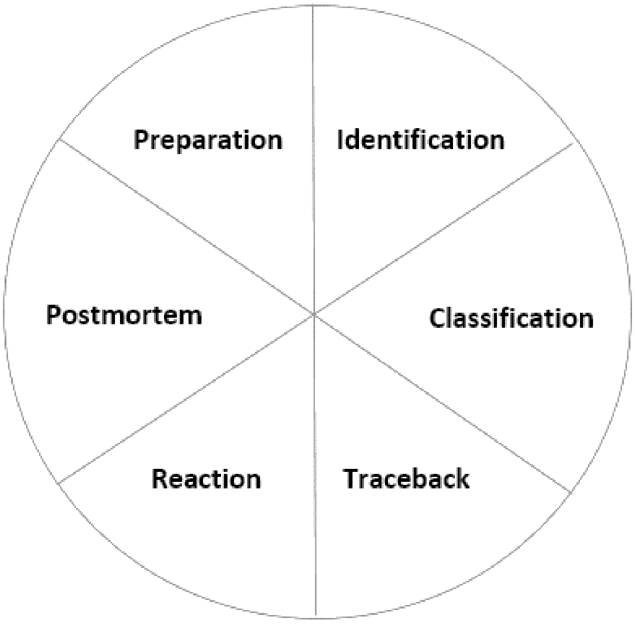


Fig. 1 Six-phase methodology proposed by Cisco

III. Categories of DDOS Attack

DDoS attacks can be categorized into three types

- Volumetric Attacks
- Application Flood Attacks
- Protocol Attack

3.1 Volumetric Attacks

In volumetric attacks, target gets flooded by continuous requests or queries. When internet service and network equipment is not able to respond to the packets or receive any more requests then is starts denying every request it receive and soon even the legitimate users will no longer be able to access the service it requested.

Recent DDoS attacks have scaled up so big that they can create traffic over 1TB/Sec. The methodology behind volumetric attack can results in traffic that originates from heterogeneous sources. Volume based DDoS attacks are hard to detect and mitigate as traffic is not originate from a single source.

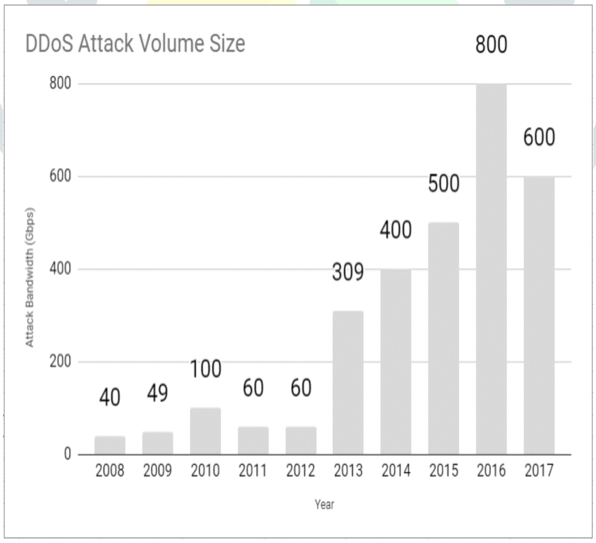


Fig. 2 Scale and target of DDoS Attack since 2008

3.2 Application based DDoS attacks

Application based DDoS attacks targets applications. HTTP floods tries to overwhelm Web servers and services. These attacks are more effective as they don't rely on high network. An attacker can generate multiple HTTP GETs or POSTS to server based on various operating system consists of legitimate requests and it is measured in Requests per second.

3.3 Protocol attack

It includes of smurf attack and SYN floods. It uses protocol based approach to create fragmented packet attacks, one of the most common and simple yet effective method of DDoS attack is Ping of Death. These attacks operates by eating up the network and server resources it slow down the working of firewalls and load balancer and it is measured in packets per second.

Denial of service attack is not limited to a large group of bots sending and requesting packets in order to choke down the network system, but there is completely another approach for executing denial of service attack called slow denial of service attack.

Service	Port	Protocol	Attacks
Reserved (icmp)	0	ICMP	444
Microsoft-ds	445	TCP	3984
Netbios	135	TCP	349
Netbios	139	TCP	3968
http	80	TCP	722
telnet	23	TCP	16
ssh remote login	22	TCP	52
ms-sql	1435	UDP	118
Unassigned	1026	UDP	3883
Unassigned	1027	UDP	3865
Unassigned	1028	UDP	3714

Slow Denial-of-Service attack is a layer-7 protocol attack. It works by sending packets at a very slow rate. Attacker sends a "get" request to a server and request for particular file or web page. The web server might send back the required information and wait for another request from client. When it is about to end the conversation then attacker again sends a packet request, so the packets are transfer at a low bandwidth. Attacker keeps the connection going as long as possible, and then it sends similar requests with more connections.

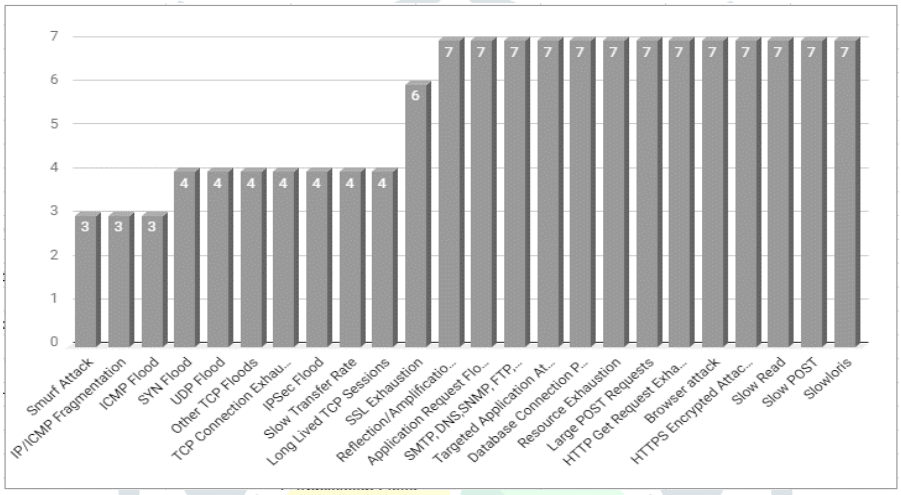


Fig. 3 DDoS Attacks against various layers of OSI model

It is very difficult for a firewall to notice this, because these are valid HTTP requests. Slowloris is one of the prime example of slow denial-of-service attack.

IV. Intrusion Detection System

When a DDoS attack happens, the detection method focuses on the detection strategies that includes detection method based on the nature and bandwidth of attack. Easiest way to oppose these attacks is to use predefined approach of using default settings of network firewall which can filters request from unauthorised users or host. However, the former mentioned method is not suitable with more advanced attacks. Firewall standalone is not the safest approach as it also attempts to tackle against the inflow of traffic that needs to be filtered. To counter this flaw we can use a separate detection system which can address the issue when it arises.

4.1 NIDS

NIDS or Network Intrusion Detection System is a type of IDS is used for monitoring incoming and outgoing traffic to detect threats. It searches for any suspicious patterns and when a fraudulent activity is detected, it signals the Network administrator. NIDS utilizes switches, routers or firewall for analyzing the packets.

3.2 HIDS

HIDS or Host based Intrusion Detection System is a type of IDS can also be utilized on the host. It uses log report of client machines or host machine to detect the intrusion. It analysis the log report created by operation system and application software. If there is any suspicious pattern found then it will be treated as an attack. HIDS gives insights of event happened, what task performed.

V. Intrusion Prevention System

An Intrusion Prevention System traditionally encompasses a set of steps that the system follows if it encounters an attack and it’s also used to remove delays in responses. These techniques are employed in unison; are known as intrusion detection and prevention systems. When an attacker attacks the system and shows his interest on the specific data/folder/file then the system observes that host and deploys the Host IDPS and informs the administrators of the theft or damage done to the data. The strength of an HIDPS lies in the monitoring of the incoming and outgoing traffic and operation performed by host in system. Encrypted packets pose no difficulty to it during analysis, packets are monitored based on the destination and host address. The Network based Intrusion Detection and Prevention System can view and monitor the network traffic and informed network administrator so that attack can be detected.

Signature matching helps in creating log report of an event if there is any intrusion. In anomaly detection IDS knows the normal behaviour of system and network. If there is any abnormal activity happens that does not match with the daily traffic state then IDS treats it as an attack. Network Intrusion Detection and Prevention System uses both methods for a superior detection rate. The IPS shows a list of IP addresses that have been blocked due to inappropriate behaviour on the network traffic.

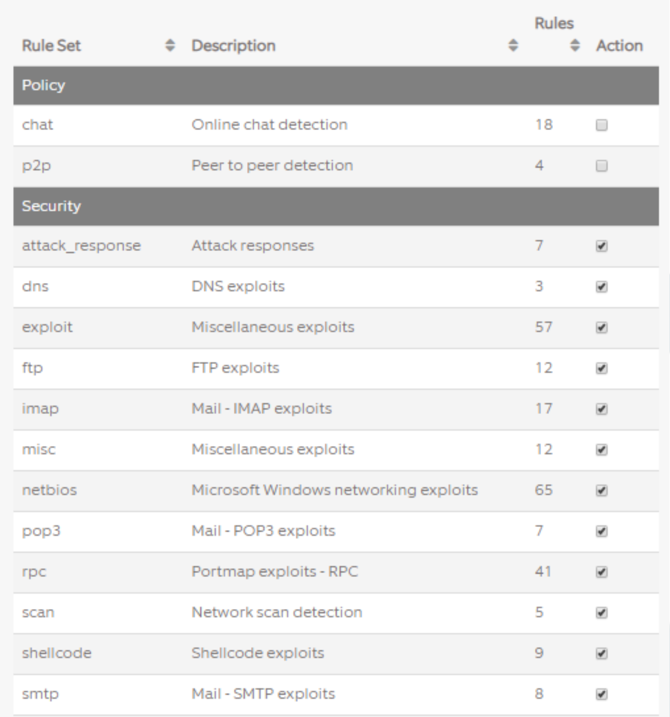
5.1 White List

White list contains a list of user IP address, port number and network address. Whitelisted addresses are those which are secure and are allowed to access the network. Administrator can delete or create a white list entry if required.

5.2 Blocked List

Blocked List or Black List is the list of IP addresses which are not allowed to send or receive any packets. Port Numbers are usually added in this list so that outsiders can be stopped from accessing the services which can result it in major security concern. Blocked host can be managed by network administrator as he/she can remove or add a user to list

SID or Security ID is the intrusion detection system ID that triggered the block. The block time can be set that is a timer can be set for limiting the network access to a particular time period. Firewall rules can be created based on requirement



Rule Set	Description	Rules	Action
Policy			
chat	Online chat detection	18	□
p2p	Peer to peer detection	4	□
Security			
attack_response	Attack responses	7	☑
dns	DNS exploits	3	☑
exploit	Miscellaneous exploits	57	☑
ftp	FTP exploits	12	☑
imap	Mail - IMAP exploits	17	☑
misc	Miscellaneous exploits	12	☑
netbios	Microsoft Windows networking exploits	65	☑
pop3	Mail - POP3 exploits	7	☑
rpc	Portmap exploits - RPC	41	☑
scan	Network scan detection	5	☑
shellcode	Shellcode exploits	9	☑
smtp	Mail - SMTP exploits	8	☑

Fig.4 Firewall Rule Set

Snort an open source tool is one of the examples of NIDPS. much like how an antivirus program works, a signature based system uses the same approach that includes configuring features in the signature database. The system then compares the previous information to present scenario, if there are similarity then packets are allowed to move in and out through firewall and IDS but if signatures are not match with the existing traffic then packets will be dropped to free up the network space. DDoS attacks usually works by eating up the network resources it consumes processor and system memory of servers by sending malformed requests. While working it does not identify normal traffic as intrusive in nature for that purpose Anomaly detection is used.

VI. Methodology

DDoS Mitigation System proposed is based on NIDS offering by ClearOS (CentOS & Red Hat Enterprise Linux). Attack Detector Module, Intrusion Detection Technique is used for detection of DDoS attacks. Traffic is diverted using routing technique for managing request load. DDoS traffic is removed out via filtering technique. Security logs are used for optimizing the network security. purposed strategy includes of Simulation & Testing Of DDoS Attacks in order to check the feasibility of system. Intrusion detection and prevention system is implemented to use DDoS Mitigation Technique efficiently and effectively to prevent or in worst case reducing the downtime of server and network resources. The proposed method to stop complex DDoS attacks in a proactive manner that does not require human intervention.

The existing techniques and methods for DDoS protection include various implementations of gateway antiphising engine, gateway antimalware, application filter, protocol filters, packet logging, and others. Other defensive techniques include, but are not limited to, port-hopping, entropy-based anomaly detection, packet monitoring, packet filtering method, and intrusion detection system using the Dempster Shafter theory. These methods were analyzed in the research.

Most of above methods are theoretical and would be difficult to implement in practice. IP traceback is very useful to detect the real source of an attack, but its implementation would require either change of TCP/IP specification, which will impact the functioning of the entire Internet, or significant changes in firmware of routers and other active network equipment of any vendors throughout the world. The proposed method can be easily implemented on practice, and the pieces of code were developed during the research process, ensuring the code can be used by developers and vendors. The Gateway Antiphishing uses a central antiphishing engine to scan web, FTP, mail and more. It protects devices connected to your network by shielding users from malicious links detected by the engine. Antiphishing engine works in order to block users from accessing phishing websites. In Phishing, attacker creates a website that look and feel like the original website. These websites are tend to steal personal information. Generally, attacker creates bank websites or other social media websites that seems trusted and when the user visits these websites and fills in the secret information required for transaction or other personal interest then this information is saved in the attackers' webserver. Attacker can use this information for gaining financial and other benefits. Content filtering and web proxy can help in securing the users from such fraud. Antimalware or a good antivirus solution can scan the system and if malware is detected then remove it.

Application and protocol filter technique can be helpful in blocking unwanted traffic. In general scenario it is possible that an employee is using a web service that is generating huge amount of incoming traffic then with the help of filtering such traffic can be blocked. Application filter enables network administrator to block harmful or 3rd party apps internet access as botnets gets installed in a user's device using these applications and filtering these applications and protocols provides an additional layer of security. In Oct 21, 2016 Mirai, malware caused the attack. Mirai worked in a non-traditional way it didn't take over the computer systems in order to create a botnet but it took the other way, it attached itself with the internet devices such as network printer, CCTV cameras, router etc. Reason behind the security breach of IoT device was the ignorance of setting secure password, generally users don't care about changing the default credentials, which leads to compromise of security. The network administrator can create certificates and has tendency to create certificate authority. Certificate Authority provides certificate for digitally signing a message or ensuring authentication during communication. Digital signature uses hash function to generate hash of data. This hash data is signed with private key of sender using signing algorithm and then on the other side receiver uses public key of sender with verification algorithm to get some output. Receiver then again uses hash function to generate hash data if it is similar to original then signature is valid. Since message is signed using private key of sender it ensures the principle of authentication and non-repudiation. Certificate Authority gives ability of self-signing of certificates. It is very secure and effective similar to SSL. Only inconvenience of self-signing is that user has no other option but to trust the certificate in order to communicate.

IV. CONCLUSION

In this work, I have presented the design and implementation of a DDoS mitigation system. During the design, implementation, and testing many interesting problems have surfaced. It is hard to prevent the DDoS on the server side, as security measure should be performed on end user side as well. Digital Signatures used for enabling encryption in the local network. Digital certificates is a trusted method for encrypting information. It is industry standard for network security. It provides authentication and sender cannot deny of sending the message afterwards. Administrator can manage the certificates. He can create as well as deploy it for authenticating users and applications. Secure Socket Layer (SSL) certificates are used globally for encrypting the information through a secure medium and it also provides authentication.

DDoS is a complex and dynamic attack type so it requires a sophisticated approach. NIDS based mitigation may provide security from DDoS attacks upto a level but in today era, attack generates GigaByte traffic per second, which is hard for an IDS/IPS System to mitigate. Hybrid DDoS Mitigation Systems can be helpful in such conditions. Intrusion Protection works efficiently by detecting fraudulent activity and taking pro-active measures for blocking such attempt to access the system, though no method is completely secure but by continual updates in security perimeter can be deployed for network. Cyber-attacks have become more sophisticated and attackers use a variety of tactic. The rapid growth of largescale DDoS attacks makes it difficult to analyse how the attack has been initiated and once it is detected, it gets even hard to resolve the attack. Global threats will require new global interventions, involving enterprises, service providers, governments and consumers. Although it is difficult to be fully prepared for any incoming threat but mitigation steps can be taken. In this research, I studied methods that are used by attackers for creating a DDoS attacks. Then I proposed methods for detecting DDoS attacks by using Multilayer Firewall and Intrusion Detection Prevention System. Gateway based antimalware; content filter and proxy are used for removing the malicious traffic. Application filter and protocol filter blocks unwanted traffic network. Individual techniques for defending against an attack may not work or give false positive result, defence mechanism works in cooperation with other techniques to provide collective increase in security of system and network resources.

There are many researches in field of DDoS mitigation. However, no effective method or solution is available that can completely resolve or block DDoS attack. Even the popular methods are not effective globally because of distributed administration of the internet.

VII. ACKNOWLEDGMENT

It is a great pleasure for me to acknowledge and express thanks to all those who helped, encouraged and guided me. I am highly grateful to Ms. Latha Banda (Associate Professor, Lingaya's Vidyapeeth, Faridabad) for providing valuable suggestions and precious time in accomplishing my project.

Finally, I express my gratitude to all who have directly or indirectly contributed to the successful completion of this project.

REFERENCES

[1] S Axelsson (2000) 'Intrusion Detection Systems: A Survey and Taxonomy', Chalmers University Tech Report, 99-15.
[2] Proctor, Paul E. The Practical Intrusion Detection Handbook. New Jersey: Prentice Hall PTR, 2001.
[3] Northcutt, Steven. Network Intrusion Detection, An Analyst's Handbook. Indianapolis:New Riders, 1999.
[4] Bace, Rebecca. "An Introduction to Intrusion Detection and Assessment: for System and Network Security Management." ICSA White Paper, 1998.
[5] G. Badishi, A. Herzberg, and I. Keidar, "Keeping denial-of-service attackers in the dark," IEEE Trans. Depend. Secure Comput., vol. 4, no. 3, pp. 191–204, Jul.–Sep. 2007.
[6] T. Peng, C. Leckie, and K. Ramamohanarao, "Detecting distributed denial of service attacks by sharing distributed beliefs," in Proc. 8th ACISP, Wollongong, Australia, Jul. 2003
[7] S. Egelman, L. F. Cranor and J. Hong, "You've been warned: An empirical study of the effectiveness of web browser phishing warnings," in CHI '08: Proceeding of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems, 2008, pp. 1065-1074.
[8] Stephen Northcutt, "Network Intrusion Detection: An Analyst's Handbook" First Edition, New Riders Publishing, June 16, 1999
[9] Ahmed, E., G. Mohay, A. Nadarajan, B. Ravindran, A. Tickle, and R. Vijayasarathy, An Investigation into the Detection and Mitigation of Denial of Service(DoS) Attacks, chapter 5. Springer, 2011. Under Publication.

[10] Aura, T., P. Nikander, and J. Leiwo, DoS-resistant authentication with client puzzles. In Lecture Notes in Computer Science. Springer-Verlag, 2000.

[11] M. Di Natale, H. Zeng, P. Giusto, and A. Ghosal. Understanding and using the controller area network communication protocol: theory and practice. Springer Science & Business Media, 2012.

[12] I. Foster and K. Koscher. Exploring controller area networks. USENIX Usenix Magazine, 40(6), 2015.

[13] T. Hoppe and J. Dittman. Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy. In Proceedings of the 2nd workshop on embedded systems security (WESS), pages 1–6, 2007.

[14] D. Hristu-Varsakelis and W. S. Levine, editors. Handbook of Networked and Embedded Control Systems. Birkhäuser, 2005.

[15] M. J. Kang and J. Kang. A novel intrusion detection method using deep neural network for in-vehicle network security. In IEEE 83rd Vehicular Technology Conference, VTC Spring 2016, Nanjing, China, May 15-18, 2016, pages 1–5, 2016.

[16] U. E. Larson, D. K. Nilsson, and E. Jonsson. An approach to specification-based attack detection for in-vehicle networks. In Intelligent Vehicles Symposium, 2008 IEEE, pages 220–225. IEEE, 2008.