A Defense Approach for Detecting State Explosion Attacks in Practical Mobile Data Offloading

J. Deepa, K. Santhi

***Abstract*— In a disruption-tolerant, reliable transport layer protocol that masks failures of a preferred network. In disruption/delay-tolerant protocols, it provides the same semantics as TCP in an IP packet level. It would also greatly reduce the phone network costs both ISPs and end users. But in malicious environments, an attacker can instruct zombie hosts to create many DTP connections with a long keep-alive duration on a target server. The application sometimes has to maintain a large buffer per request. In Defense Approach (DA) method, it detects suspicious requests by careful resource accounting and dynamically reset the keep-alive duration's when it is suspected to be under attack. Defense approach (DA) is proposed by systematically injecting protection mechanisms into the code itself. And then to denote an attack targeting a renewable resource a busy attack, and an attack targeting a non-renewable resource a claim-and-hold attack. Experimental results shows that the proposed method achieves high performance and high efficient when compared to the existing method.**

***Index Terms*—Delay Tolerant Protocol, Wi-Fi Offloading.**

I. INTRODUCTION

Wi-Fi is an originally licensed by the Wi-Fi Alliance to describe the underlying technology of Wireless Local Area Networks (WLAN) based on the IEEE 802.11 specifications. Wi-Fi was developed for mobile computing devices, such as laptops, in LANs, but is now increasingly used for more applications, including Internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras. There are even more standards in development that will allow Wi-Fi to be used by cars in highways in support of an Intelligent Transportation System to increase safety, gather statistics, and enable mobile commerce IEEE 802.11p. A person with Wi-Fi device, such as a computer, telephone, or Personal Digital Assistant (PDA) can connect to the Internet when in proximity of an access point. The region covered by one or more access points is called a hotspot. Hotspots can range from a single room to many square kilometers of overlapping hotspots. Wi-Fi can used to create a Wireless mesh network. These architectures are used in Wireless community network, municipal wireless networks like Wireless Philadelphia, and metro-scale networks like M-Taipei. Wi-Fi also allows connectivity in peer-to-peer mode, which enables devices to connect directly with each other. This connectivity mode is useful in consumer electronics and gaming applications.

Depiction of a device sending information wirelessly to another device connected to the local network, in order to print a document. Wi-Fi can be less secure than wired connections (such as Ethernet) because an intruder does not need a physical connection. Web pages that use SSL are secure but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The early encryption WEP, proved easy to break. Higher quality protocols (WPA, WPA2) are added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), and had a serious flaw that allowed an attacker to recover the router's password. The Wi-Fi Alliance has since updated its test plan and certification program to ensure all newly certified devices resist attacks.

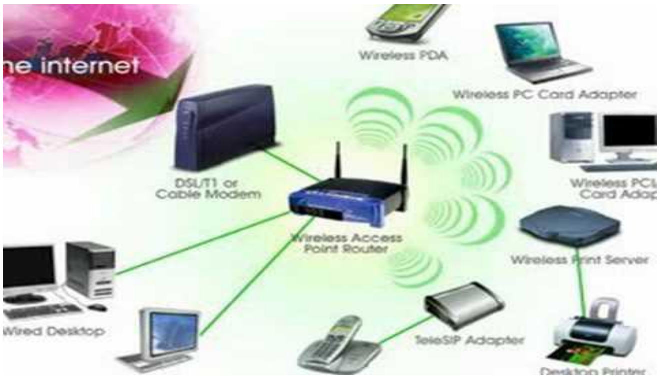


Figure 1 Wi-Fi Architecture

A. *ADVANTAGES AND LIMITATIONS OF WI-FI NETWORK*

a) ADVANTAGES

Wi-Fi allows cheaper deployment of Local Area Networks (LANs). such as outdoor areas and historical buildings, can host wireless LANs. Manufacturers are building wireless network adapters into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices. Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service. Wi-Fi Protected Access encryption (WPA2) is considered secure, provided a strong passphrase is used. New protocols for quality-of-service (WMM) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video). Power saving mechanisms (WMM Power Save) extends battery life.

b) LIMITATIONS

Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels beyond those permitted in the US for the 2.4 GHz band (1–13 vs. 1–11), while Japan has one more on top of that. A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or

J.Deepa, Research Scholar, Department of computer science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, 9659069207

K.Santhi, Associate Professor, Department of Computer science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore.,

more, such as 2 and 7, do not overlap. The oft-repeated adage that channels 1, 6, and 11 are the only non-overlapping channels is, therefore, not accurate. The current 'fastest' norm, 802.11n, uses double the radio spectrum/bandwidth (40 MHz) compared to 802.11a or 802.11g (20 MHz). This means there can be only one 802.11n network on the 2.4 GHz band at a given location, without interference to/from other WLAN traffic. 802.11n can also be set to use 20 MHz bandwidth only to prevent interference in dense community. Many newer consumer devices support the latest 802.11ac standard, which uses the 5 GHz band and is capable of multi-station WLAN throughput of at least 1 gigabit per second. According to a study, devices with the 802.11ac specification are expected to be common by 2015 with an estimated one billion spread around the world**.**

B. APPLICATIONS OF WI-FI NETWORK

To connect to a Wi-Fi LAN, a computer has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a station. All stations share a single radio frequency communication channel. Transmissions on this channel are received by all stations within range. The hardware does not signal the user that the transmission was delivered and is called a best-effort delivery mechanism. A carrier wave is used to transmit the data in packets, referred to as "Ethernet frames". Each station is constantly turned in on the radio frequency communication channel to pick up available transmissions.

a) Internet access

A Wi-Fi enabled device can connect to the Internet when within range of a wireless network which is configured to permit. The coverage of one or more (interconnected) access points called hot spots can extend from an area so small in few rooms to so large in many square kilometers. Coverage in the larger area may require a group of access points. Outdoor public Wi-Fi technology is successfully in wireless mesh networks in London, UK. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access.

b) Campus-wide Wi-Fi

Many college campuses in the United States provide at least partial wireless Wi-Fi Internet coverage. Carnegie Mellon University built the first campus-wide wireless Internet network, called Wireless Andrew, at Pittsburgh campus in 1993 before Wi-Fi branding originated. In Europe many universities collaborate in providing Wi-Fi access to students and staff through the eduroam international authentication infrastructure.

c) Direct computer-to-computer communications

Wi-Fi allows communication directly from one computer to another without an access point intermediary. This is called *ad hoc* Wi-Fi transmission. In these wireless ad hoc network mode has proven popular with multiplayer hand held game consoles, such as Nintendo DS, PlayStation Portable, digital cameras, and other consumer electronics devices. Some devices can also share their Internet connection using ad hoc, becoming hotspots or "virtual routers".

II. DELAY TOLERANT PROTOCOL

The explosive popularity of smart phones and mobile devices drives massive growth in the wide-area mobile data communication. Many mobile applications either depend on ad-hoc downloading resumption mechanisms or redundantly re-transfer the same content when disruptions happen. The design and implementation of DTP, a disruption tolerant transport layer protocol is presented that transparently masks network failures from the application layer. Unlike previous disruption/delay-tolerant protocols, DTP provides the same semantics as TCP on an IP packet level when the mobile device is connected to a network while providing the illusion of continued connection even if the underlying physical network becomes unavailable.

On a high level, DTP works similarly to TCP when the mobile device is attached to a network but it provides the illusion of continued connection to the applications even when the underlying network is unavailable. This way, DTP allows the mobile applications to exploit Wi-Fi offloading without requiring them being DTN-aware. The key technical challenge in DTP is how manage the connection when the physical network switches between on and off. Instead of binding the connection on the four connection tuples, DTP binds the connection to a flow ID that is agreed at the initial connection setup time and does not change during the connection lifetime. When a mobile host moves to another network, it can resume the connection with a new IP address and a port number by cryptographically attesting that it owns the flow ID of the connection. The DTP connection closes either when both parties explicitly tear it down or when the keep-alive duration of the connection expires. The keep-alive duration is the estimated connection lifetime set at the connection setup time that can be updated during the course of the connection.

A. Disadvantages of DTP

- ➢ In malicious environments, an attacker can instruct zombie hosts to create many DTP connections with a long keep-alive duration on a target server,
- ➢ Maintain a large buffer per request because a client sends large-file request and goes offline immediately afterwards.
- ➢ Less efficient.

III. DEFENSE APPROACH

In the proposed research, in order to detect suspicious requests, defense approach (DA) is proposed by systematically injecting protection mechanisms into the code itself. In DA approach, first annotate the code and these annotations serve as both sensors and actuators: watching for resource abuse and taking the appropriate action should abuse be detected.

When characterizing State explosion attacks, it is helpful to distinguish between two types of resources: renewable resources, such as CPU cycles, the bandwidth of network, disks, and buses; and non-renewable resources, such as processes, ports, buffers, PCBs, and locks. To denote an attack targeting a renewable resource a busy attack, and an attack targeting a non-renewable resource a claim-and-hold attack.

IV. Defensive Method

Overall strategy is to separate resources among activities in a program along two dimensions. For renewable resources, we balance resource usage among program functionalities, thereby confining the impact of an attack to the individual service being attacked. For non-renewable resources, we identify principal's that hold non-renewable resources and reclaim resources from principals that are not making minimal progress.

There are two defense approaches are used which is called Busy Attack Defense and Claim-and-Hold Attack Defense.

A. Busy Attack Defense

The strategy is to balance resource usage among program functionalities, thereby confining the impact of an attack to the individual service being attacked. Towards this end, introduce the concept of service and propose a resource control mechanism with actuators at service entries and sensors at resource access points.

a) Services and Resources

A *service* is a program component that provides an *independent* functionality. Each service in turn consumes some amount of renewable resources. Figure 2 shows the conceptual model of a server program divided into services. Client requests are served by different services, as they execute a code path through the program, and multiple services share various resources.

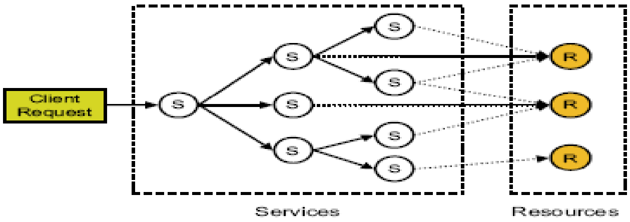
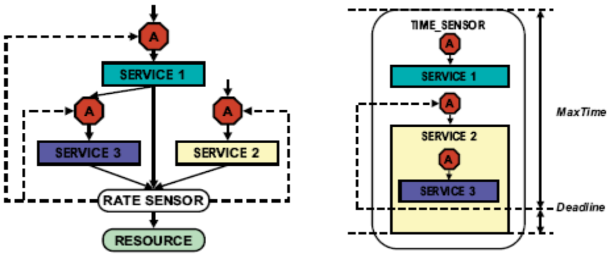


Figure 2: Service View of a Program

b) Sensor and Actuators

A systematic way to place sensors and actuators in a program, because placing them in an ad hoc way may leave holes to be exploited the code path being attacked might not have an annotation on it. On the other hand to minimize the number of annotations, especially actuators, because switching out of a code path needs to be handled in a program specific way and it takes programmer's effort to write such a handler. We found that actuators and sensors need to be placed at different locations in the program, in order that (1) actuation happens at the right place, and (2) resource usages to be properly limited.



(a) Rate Control (b) Time Control

Figure 3: Managing Renewable Resources

B. Claim and Hold Attack Defense

In order to consume renewable resources, the attacking activity must be *active*, i.e., executing code on the CPU. This observation has greatly simplified the solution to defend busy attacks basically need to control the execution frequency and duration of different code paths. Protecting non-renewable resources is essentially a process of specifying a replacement policy: when the resource becomes exhausted, which ones should be reclaimed. Resources can be reclaimed either periodically or when some event indicates recycling is necessary. Thus, the problem boils down to one of deciding: (1) what resources to reclaim, and (2) when to reclaim them. The two metrics are used progress and pressure that characterize these two aspects of a replacement policy, respectively. The defense strategy involves annotating a program with sensors and actuators that set and react to these two metrics.

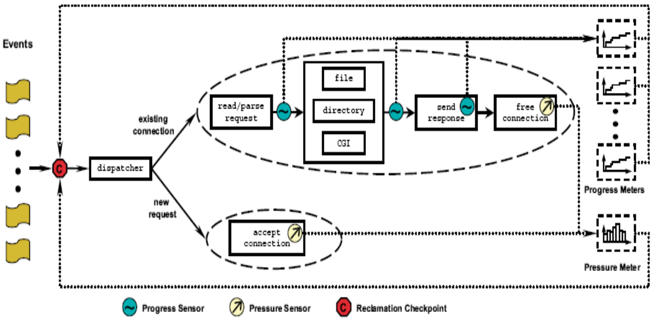


Figure 4: Managing Non-renewable Resources

a) Progress and Pressure

The problem with this approach is that it is biased against clients on a slow link or those downloading a large file. A better solution is to measure how well a client is making use of the resources it has acquired, and combine this information with other metrics such as age. A client should be allowed to hold resources longer than others, as long as it has a good reason. We use progress to denote such a metric. Progress is expected to increase proportionally with time. A replacement policy also has to specify when to reclaim resources. One can annotate a program with a progress sensor that records how many bytes have been read or written, how many packets have been forwarded. Since recycling itself could be an expensive operation, uncontrolled invocations also open up the possibility of busy attacks.

Define a pressure metric to control the invocation of the reclaim function. A resource should be recycled when the pressure on it exceeds a certain threshold, which could be caused either by too many clients requesting the resource, or no clients releasing the resource.

b) Advantages of DA

- Highly efficient
- Detect suspicious requests
- High performance

c) Comparison graphs

Time

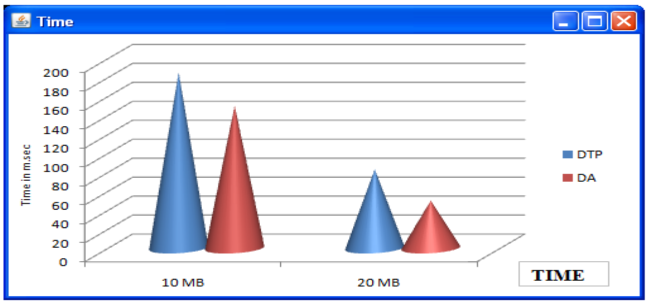


Figure 5 Time Performance

Cost

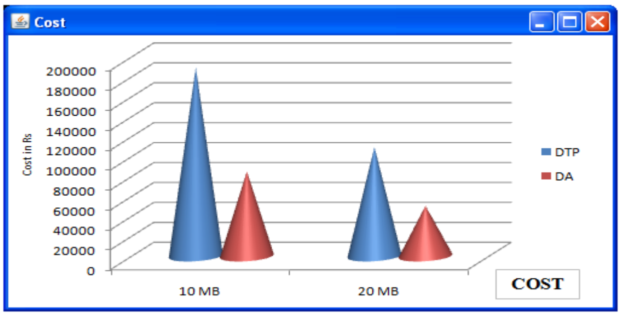


Figure 6 Cost

V. CONCLUSIONS

While many works have shown the effectiveness of Wi-Fi mobile data offloading, there has not been a practical data delivery mechanism to support it. A DTP, disruption-tolerant reliable transport layer protocol is presented which allows seamless switching between 3G and Wi-Fi networks on the same connection for mobile applications. To design a migrate existing applications to transparently recover from network disruptions, with little performance degradation from that of TCP. But in malicious environments, an attacker can instruct zombie hosts to create many DTP connections with a long keep-alive duration on a target server. So, a defense method is used to detect suspicious requests by careful resource accounting and dynamically reset the keep-alive durations when it is suspected to be under attack.

VI. FUTURE WORK

Malicious and selfish behaviors represent a serious threat against routing in delay/disruption tolerant networks (DTNs). However, note that this sort of attack is not unique to DTP but can be launched on any UDP-based servers using different attacks. This can be considering in future work.

REFERENCES

[1] J. Mitola III and G. Q. Maguire Jr. Cognitive Radio: Making Software Radios More Personal. IEEE Personal Communications, 6(4):13–18, 1999.

[2] A. Balasubramanian, R. Mahajan, and A. Venkataramani. Augmenting Mobile 3G Using WiFi. In Proceedings of ACM MobiSys, 2010.

[3] K. Lee, I. Rhee, J. Lee, S. Chong, and Y. Yi. Mobile Data Offloading: How Much Can WiFi Deliver? In Proceedings of ACM CoNEXT, 2010.

[4] J. Scott, P. Hui, J. Crowcroft, and C. Diot. Haggle: A Networking Architecture Designed Around Mobile Users. In Proceedings of IFIP WONS, 2006.

[5] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott. Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms. In Proceedings of IEEE INFOCOM, 2006.

[6] K. Fall. A Delay-Tolerant Network Architecture for Challenged Internets. In Proceedings of ACM SIGCOMM, 2003.

[7] S. Burleigh, M. Ramadas, and S. Farrell. Licklider Transmission Protocol - Motivation. RFC 5325, IETF, 2008.

[8] S. Farrell, M. Ramadas, and S. Burleigh. Licklider Transmission Protocol - Security Extensions. RFC 5327, IETF, 2008.

[9] K. Scott and S. Burleigh. Bundle Protocol Specification. RFC 5050, IETF, 2007.

[10] K. Jang, S. Han, S. Han, S. Moon, and K. Park. SSLShader: Cheap SSL Acceleration with Commodity Processors. In Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2011.

[11] Y. Gu and R. L. Grossman. UDT: UDP-based Data Transfer for High-Speed Wide Area Networks. Computer Networks (Elsevier), 51(7), 2007.

[12] R. Yanggratoke, A. Azfar, M. J. P. Marval, and S. Ahmed. Delay Tolerant Network on Android Phones: Implementation Issues and Performance Measurements. Journal of Communications, 6, 2011.

[13] V. Cerf, S. Burleigh, L. Torgerson, R.Durst, K. Scott, K. Fall, and H. Weiss. Delay-Tolerant Networking Architecture. RFC 4838, IETF, 2007.

[14] A. Myles, D. Johnson, and C. Perkins. A mobile host protocol supporting route optimization and authentication. IEEE Journal on Selected Areas in Communications, 13(5), 1995.

[15] A. C. Snoeren and H. Balakrishnan. An end-to-end approach to host mobility. In Proceedings of ACM MOBICOM, pages 155–166, 2000.

[16] R. Moskowitz and P. Nikander. Host Identity Protocol Architecture. RFC 4423, IETF, 2006.

[17] S. Farrell, V. Cahill, D. Geraghty, I. Humphreys, and P. McDonald. When TCP Breaks: Delay- and Disruption-Tolerant Networking. IEEE Internet Computing, 10(4), 2006.

[18] R. E. Brown. Impact of Smart Grid on distribution system design. IEEE, Power and Energy Society general Meeting, 2008.

[19] SEO Updates. Mobile vs Desktop Internet Usage Stats 2011,2011, http://www.seodailyupdates.com/2011/06/mobile-vs-desktop-internet-usage-stats.html.

[20] CISCO. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015. Technical report, 2011.

[21]KT.ollehWiFizone Finder.http://zone.wifi.olleh.com/en/index.action.

[22] Podcast. http://www.apple.com/itunes/podcasts/.

[23] DoggCatcher. http://www.doggcatcher.com/.

[24] TubeMate. http://tubemate.tistory.com/.

[25] Dropbox. https://www.dropbox.com/.

[26] Google/Ipsos OTC MediaCT. The Mobile Movement Study, 2011.

[27] Android Market. https://market.android.com/.

[28] MapDroyd. http://www.mapdroyd.com/.

[29]Beyondpod. http://www.beyondpod.mobi/android/index.htm.

[30]GoogleListen.https://market.android.com/details?id=com.google.android.apps.listen/.

[31] Winamp. http://www.winamp.com/android/.

[32] GNU wget. http://www.gnu.org/s/wget/.