

On Security in TCP/IP over Wireless Network

Shamila Makki
Electrical and Computer
Engineering Department
Florida International University
Miami, FL, U.S.A.

Subbarao V. Wunnava
Electrical and Computer
Engineering Department
Florida International University
Miami, FL, U.S.A.

Abstract - *The Transmission Control Protocol/Internet Protocol (TCP/IP) is combination of different protocols at various layers. TCP/IP is the basic communication language or protocol of the Internet and private networks either an intranet or an extranet. TCP interfaces between the application layer and the network layer. It is a connection oriented, reliable delivery transport layer protocol that sends data as an unstructured byte stream. It is responsible for verifying the correct delivery of data from client to server. IP is a very simple protocol and demands only minimal functionality from the underlying medium and can be deployed on a wide variety of network. It is responsible for moving packet of data from node to node. Security requirements for wireless communications are similar to the wired network but are treated differently because of applications involved and possible fraud. In this paper we investigate and analyze TCP/IP over wireless network and compare it with TCP/IP over wired networks. We will also discuss security issues related to the deployment of TCP/IP protocols over wireless networks.*

Keywords: Internet Protocol (IP), Transmission Control Protocol (TCP), Security, Congestion

1.0 Introduction

TCP/IP created from a simple set of protocols. TCP/IP protocol suite is so named for two of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP) [1]. TCP/IP is the engine for the Internet and all the applications on the Internet make use of TCP, relying upon its system that ensures safe delivery of data across an unreliable IP layer. TCP/IP is independent of any particular transmitting medium. TCP/IP is not secure against data snooping, connection hijacking, authentication attacks, or other network security threats [2]. Losses of wireless link have bad impact on TCP performance due to the complexity in distinguishing congestion losses from wireless link losses [3].

The wireless networks are less reliable and have extremely different characteristics than the wired networks, which are composed of copper or fiber optic cable and provide reliable communication between hosts. TCP provides reliability by maintaining a running average of estimated round-trip delay and mean deviation, and by retransmitting any packet whose acknowledgement is not received within twice the deviation from the average. Due to the relatively low error rates over wired networks packet losses are assumed to be as a result of congestion [4].

Wireless links are distinguished by low bandwidth and high bit-error rates and time-varying. Originally TCP was developed for wired networks and because of the difference in bit-error rates causes a major loss in the performance of TCP.

Security requirements for wireless communications are similar to the wired network but are treated differently. Security is required for different parts of the wireless networks. In addition to the security

requirements for the wireless networks there are also some security requirements that are specific to TCP/IP.

The structure of this paper is as follows, after a brief introduction in section 1; we review the related work in section 2, and describe the TCP performance over wireless networks in section 3. Then in section 4, we compare the TCP/IP over wired and wireless networks. In section 5, we discuss the security in wireless network. In section 6, we introduce the TCP/IP specific security and finally we conclude the paper in section 7.

2.0 Related Works

This section reviews previous work on improving TCP performance over wireless networks. TCP is a reliable transport protocol adjusts to work with traditional networks with low bit-error rates and stationary hosts. Therefore its performance will be decreased with wireless links and mobile hosts that have higher bit-error rates [5].

Reference [6] describes the design and implementation of a simple protocol, called the snoop protocol that improves TCP performance in wireless networks. The protocol modifies network-layer software mainly at a base station and preserves end-to-end TCP semantics. The main idea of the protocol is to cache packets at the base station and perform local retransmissions across the wireless links. Simulations of this protocol show that it is significantly more robust to deal with unreliable wireless links as compared to normal TCP. This enables the protocol to tolerate at least 10 times as high an error rate without any performance degradation.

Chan *et al.* [7] have comprehensively evaluated the impact of variable rate and variable delay on long-lived TCP performance. They proposed a model to explain and predict TCP's throughput over a link with variable rate and/or delay. They have also proposed a network-based solution called Ack Regulator that mitigates the effect of variable rate and/or delay without significantly increasing the round trip time, while improving TCP performance by up to 40%.

Reference [8] uses reliable transport protocols such as TCP use end-to-end flow, congestion and error control mechanisms to provide reliable delivery over an internet-work. Though, the end-to-end performance of a TCP connection can suffer considerable degradation in the presence of a wireless link. They explored alternatives for optimizing end-to-end performance of TCP connections across an internet-work consisting of both fixed and mobile networks. The central idea in their approach is to transparently split an end-to-end connection into two separate connections; one over the wireless link and the other over the wired path. The connection over the wireless link may either use regular TCP or a specialized transport protocol optimized for better performance over a wireless link. Their approach did not require any changes to the existing protocol software on stationary hosts. Results of a systematic performance evaluation using both their approach and regular TCP showed that their approach yields some significant performance improvements.

3.0 TCP Performance over Wireless Links

TCP is the most common transport protocol. It can regulate end to end delays and packet losses caused by congestion. TCP provides reliability by sustaining a running average of estimated round-trip delay and mean deviation, and by retransmitting any packet whose acknowledgment is not received within twice the deviation from the average [9].

Wireless links has high bit-error rates and discontinuous connectivity characteristic thus all losses that are due to congestion become relatively problematic over wireless links. TCP reacts to packet losses as it

would in the wired environment: it drops its transmission window size before retransmitting packets, avoidance mechanisms [10] and resets its retransmission timer [11]. These measures result in an unnecessary reduction in the link's bandwidth utilization, thus causing a major degradation in performance in the form of poor throughput and very high interactive delays [12].

TCP performance over wireless links provides reassembly of user data and handles flow and congestion control. When a session becomes idle or acknowledgements are lost TCP detects losses using timeouts. Congestion occurs when routers are overloaded with traffic that causes their queues to build up and ultimately over flow leading to delays and packet losses. Sending window size decreases thus reducing data throughput.

When a TCP packet is lost after crossing some wireless links in the path, its retransmission has to cross those links again, thus wasting bandwidth [13]. Losses have more clear impact on paths with higher end-to-end delay, which need TCP to sustain large transmission windows to keep data flowing. On such paths TCP also suffers from false timeouts, that is, timeout, which would be avoided if the sender waited longer for acknowledgements.

4.0 Comparison of TCP/IP over wired and wireless networks

4.1 Wired networks

- High bandwidth (about 100Mbps)
- Random packet loss is negligible
- High performance rate

4.2 Wireless networks

- Reduced bandwidth
- Higher loss rate due to its vulnerability to interference and disconnection
- Low performance rate

5.0 Security in wireless network

Wireless networks share many common characteristics with wired line networks (e.g. public switch telephone/ data networks), therefore many security issues with the wired line networks apply to wireless network. Wireless channels are open system therefore this makes a wireless system more exposed to unauthorized access and manipulation of sensitive data than wired networks.

For combination of security features into wireless communication must consider restrictions that may apply to their use such as small packet size, low bandwidth, high transmission costs, limited processing and storage resources and real time constraints [14].

5.1 Common attacks against security

A network environment is in general susceptible to a number of security threats as flows [15]:

- Unauthorized use of resources
- Repudiation of actions
- Wire tapping
- ID spoofing
- Denial of Service

- Guessing of passwords
- Guessing of keys
- Viruses

5.2 Operating System – Specific Security

Many of the security features available for TCP/IP are based on those available through the operating system and it consists of the following major components [16]:

- Access Control, the security procedure for networking is an extension of the security policy for the operating system and it is as follows
 - User authentication is provided at the remote host by a user name and password.
 - Connection authentication is provided to ensure that the remote host has the expected Internet Protocol (IP) address and name.
 - Data import and export security, permits data at a particular security level to flow to and from network interface adapters at the same security and authority levels.
- Auditing, network auditing is provided by TCP/IP, using the audit subsystem to audit both Kernel network routines and application programs. The following types of events are audited [16].
 - **Kernel Events:**
Change Configuration, Change host ID, Change route, Connection, Create socket, Export object, Import object
 - **Application Events:**
Access the network, Change configuration, Change host ID, Change static route, Configure mail, Connection, Export data, Import data, Write mail to file.

6.0 TCP/IP Specific Security

In the past, there were different encoding protocols used between the terminal and the WAP gateway and between the WAP gateway and the network. TCP/IP enables the usage of TSL (Transport Security Layer) all the way from the terminal to the origin server [17]. There are some security methods (TCP/IP commands and TCP/IP trusted process) specific to TCP/IP and they work together with the operating system security features as were discussed to provide the security for TCP/IP [16]. Since TCP/IP is an open protocol the hackers find it an easy prey to attacks. Many of these attacks generate large volumes of TCP/IP traffic.

6.1 Procedure for providing various degrees of security

The following methods are generally used to provide various degrees of security [15]:

- IP filtering
- Network Address Translation (NAT)
- IP Security Architecture (IPsec)
- Secure Sockets Layer (SSL)
- Application proxies
- Firewalls
- Kerberos and other authentication systems
- Secure Electronic Transactions (SET)

6.2 Operating system security

- Trusted Path, prevent unauthorized programs from reading data from a user terminal.
- Trusted shell feature (tsh), executes only trusted programs that have been tested and verified as secure.
- Secure Attention Key (SAK), establishes the environment necessary for secure communication between user and the system.

6.3 TCP/IP Command Security

TCP/IP commands (ftp, rexec and telnet) provide a secure environment during operation [16].

- ftp function provides security during file transfer.
- rexec command provides a secure environment for executing commands on a foreign host.
- telnet function provides security for login to a foreign host.

6.4 Trusted Processes

Trusted program or trusted process is a shell script, a daemon, or a program that meets a particular standard of security. Trusted programs are trusted at different levels [16].

7.0 Conclusions

TCP/IP is an established industry standard technology and it was developed based on wired links and stationary host. TCP/IP will enable faster connections and increased efficiency for large data sizes. The performance of TCP/IP is to focus on either the transport layer or the link layer to improve the throughput.

TCP/IP performance decreases in wireless link and mobile host that have higher bit-error rates. In recent years wireless network services have found an important role in telecommunication and security is one of the critical issues for both users and providers. Open nature of wireless channels makes a wireless system more vulnerable to threats also mobile applications have particular necessities and vulnerabilities; therefore, they need exceptional security mechanism. The main constraints for providing security in mobile and wireless systems and wired system are bandwidth, memory and processing power. Many of the security features available for TCP/IP are based on the available operating system.

In the near future, wireless networks will increase extremely and there will be additional request for faster data rates, better quality of service and security. Therefore, it will require developing collaboration between different protocol layers, security mechanisms and new solutions for better transmission of data.

8.0 References

- [1] D. E. Comer, "Internetworking with TCP/IP Principles, Protocols, and Architectures", Vol.1, Prentice Hall, Upper Saddle River, N.J., 2000.
- [2] M. Strebe, C. Perkins, "TCP/IP from a Security Viewpoint", Microsoft TechNet, <http://www.microsoft.com/technet/prodtechnol/winntas/maintain/tcpip.mspx>.
- [3] G. T. Nguyen, R. H. Katz, B. Noble, M. Satyanarayanan, "A Trace-based Approach for Modeling Wireless Channel Behavior", In Proceedings of the Winter Simulation Conference, pp. 597-604, December 1996.
- [4] S. Goel, D. Sanghi, "Improving TCP Performance over Wireless Links", TENCON '98. IEEE Region 10 International Conference on Global Connectivity in Energy, Computer, Communication and Control, 1998.

- [5] D. C. Clark, V. Jacobson, J. Romkey, H. Salwen, "An analysis of TCP Processing Overhead", IEEE Communication Magazine, June 1989.
- [6] E. Amir, H. Balakrishnan, S. Seshan, R.H. Katz, "Efficient TCP over Networks with Wireless Links", In Processing HotOS-V, May 1995.
- [7] M.C. Chan, R. Ramjee, "TCP/IP Performance over 3G Wireless Links with Rate and Delay Variation", MOBICOM'02, September 2002.
- [8] R. Yavatkar, N. Bhagawat, "Improving end-to-end performance of TCP over mobile internet-works", In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pp.146-152, December 1994.
- [9] J. B. Postel, "Transmission Control Protocol", RFC, SRI International, Menlo Park, CA, RFC-793, September 1981.
- [10] V. Jacobson, "Congestion avoidance and control", In SIGCOMM88, August 1988.
- [11] P. Karn, C. Partridge, "Improving Round-Trip Time Estimates in Reliable Transport Protocols", In SIGCOMM 87, August 1987.
- [12] R. Caceres, L. Iftode, "Improving the Performance of Reliable Transport Protocols in Mobile Computing Environments", IEEE JSAC, 13(5), June 1994.
- [13] G. Xylomenos, G.C. Polyzos, "TCP and UDP Performance over a Wireless LAN", Proc. IEEE INFOCOM '99, pp.439-446, March 1999.
- [14] A. DeSimone, M.C. Chuah, O.C. Yue, "Throughput Performance of Transport-layer Protocols over Wireless LANs", Proc. IEEE GLOBECOM '93, pp. 542-549, December 1993.
- [15] A. Rodriguez, J. Gatrell, J. Karas, R. Peschke, "TCP/IP Tutorial and Technical Overview", International Technical Support Organization, August 2001.
- [16] TCP/IP, "System Management Guide: Communications and Networks", http://www.unet.univie.ac.at/aix/aixbman/commadm/tcp_security.htm.
- [17] Transition to Mobile Applications over TCP/IP, NOKIA Connecting People, White Paper. http://nds2.ir.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/tcpip_whitepaper_.pdf