RESEARCH PAPER

Enhancing SCADA System Security through IPv6 Migration

Dr. D.R.V.A.Sharath Kumar[1*], Mr.Dakey Sudhir Nageswara Rao[2], Mr.K.Narasimha Rao[3], Dr.Y. Laxmi Narasimha Rao[4]

[1*]Associate Professor, ECE Department, MVSR Engineering College, Nadergul, Hyderabad, Email: drvask_ece@mvsrec.edu.in
[2]Assistant Professor, ECE Department, MVSR Engineering College, Nadergul, Hyderabad, Email: sudhir_ece@mvsrec.edu.in
[3]Assistant Professor, ECE Department, MVSR Engineering College, Nadergul, Hyderabad, Email: narasimharao_ece@mvsrec.edu.in
[4]Assistant Professor, EEE Department, MVSR Engineering College, Nadergul, Hyderabad, Email: ylnrao_eee@mvsrec.edu.in

***Abstract*--** Supervisory control and data acquisition (SCADA) systems refer to industrial control systems (ICS): computer systems that monitor and control industrial, infrastructure, or facility-based processes. The tremendous increase in the number of network connections to the SCADA systems has made the network more susceptible to attacks by hackers. The vendors of SCADA and control products have been addressing the issues related to the security threats posed for the existing SCADA systems. The IP addressing scheme that is presently used is IPV4 and the number of addresses have almost come to an exhaustion stage and this demands the need for implementation of IPV6 throughout the world. The IPV6 has more security features and it supports almost any platform of operating system. In addition the IPV6 address has a length of 128 bits and it is possible to generate about 3.4×10^{38} addresses. In this paper, the migration to IPV6 for the security of SCADA systems has been proposed.

***Index terms*—IPV4**, IPV6, Migration, SCADA
How to cite this article: Sharath Kumar DRVA, Nageswara Rao DS, Narasimha Rao K, Laxmi Narasimha Rao Y. Enhancing SCADA System Security through IPv6 Migration. Int J Drug Deliv Technol. 2026;16(17s): 910-917. DOI: 10.25258/ijddt.16.17s.106

I. INTRODUCTION

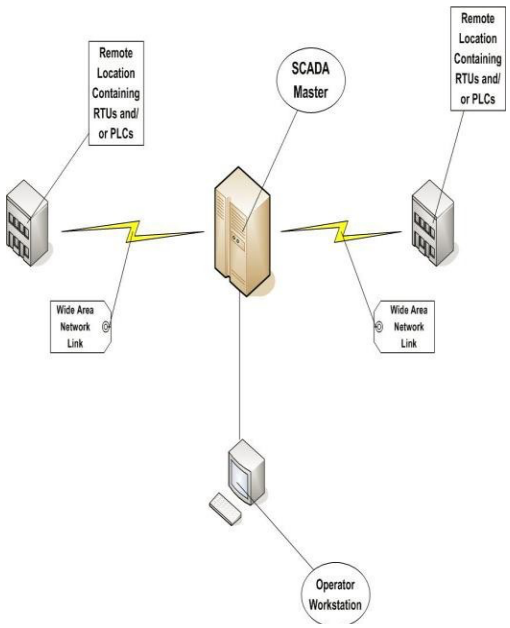


Fig 1: A typical SCADA system

A typical SCADA system is shown in Fig1 and usually consists of the following subsystems [1]: 1. A human–machine interface or HMI is the apparatus which presents process data to a human operator, and through this, the human operator monitors and controls the process.2.
A supervisory (computer) system, gathering (acquiring) data on the process and sending commands (control) to the process.3.(RTUs) connecting to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system.4.Programmable logic controller (PLCs) used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.5.Communication infrastructure connecting

*Author for Correspondence: drvask_ece@mvsrec.edu.in

the supervisory system to the remote terminal units.6.Various process and analytical instrumentation.

Communication infrastructure and methods

SCADA systems have traditionally used combinations of radio and direct wired connections, although SONET / SDH is also frequently used for large systems such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry. Some users want SCADA data to travel over their pre-established corporate networks or to share the network with other applications.

SCADA protocols are designed to be very compact. Many are designed to send information only when the master station polls the RTU. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP.

Although some believe it is good security engineering practice to avoid connecting SCADA systems to the Internet so that the attack surface is reduced, many industries, such as wastewater collection and water distribution, have used existing cellular networks to monitor their infrastructure along with internet portals for end-user data delivery and modification. Cellular network data is encrypted before transmission over the Internet.

With increasing security demands (such as North American Electric Reliability Corporation (NERC) and critical infrastructure protection (CIP) in the US), there is increasing use of satellite-based communication. This has the key advantages that the infrastructure can be self- contained (not using circuits from the public telephone system), can have built-in encryption, and can be engineered to the availability and reliability required by the SCADA system operator. Earlier experiences using consumer-grade VSAT were poor. Modern carrier-class systems provide the quality of service required for SCADA.[2] RTUs and other automatic controller devices were developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols. Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base.

II. BACKGROUND

SCADA systems have evolved through 3 generations as follows:

A. First generation: Monolithic

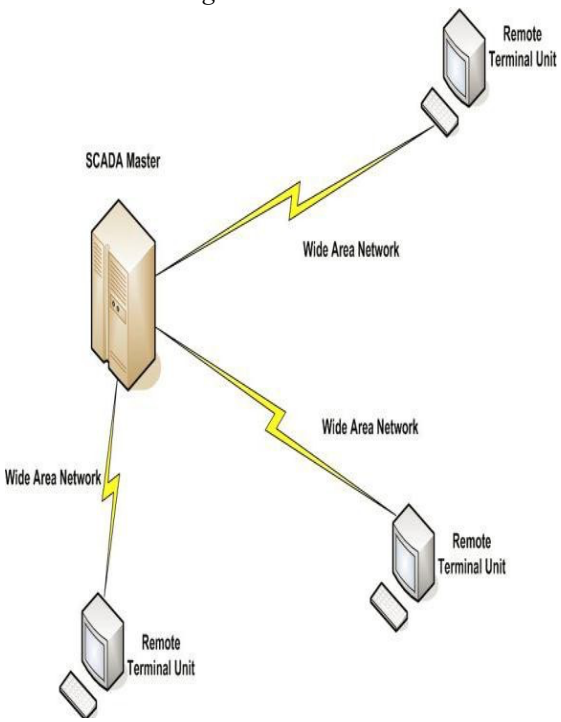


Fig 2: First generation SCADA Architecture

In the first generation SCADA Architecture [5] computing was done by mainframe computers. Networks did not exist at the time SCADA was developed. Thus SCADA systems were independent systems with no connectivity to other systems.

Wide Area Networks were later designed by RTU vendors to communicate with the RTU. The communication protocols used were often proprietary at that time. The first-generation SCADA system was redundant since a back-up mainframe system was connected at the bus level and was used in the event of failure of the primary

mainframe system.

B. Second generation: Distributed

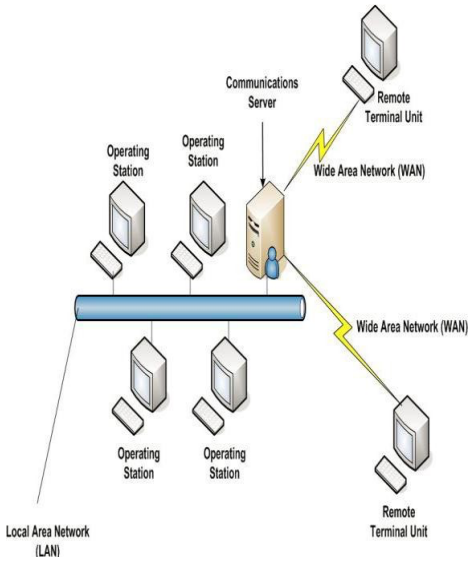


Fig 3: Second ge neration SCADA Architecture

The processing [5] will be distributed across multiple stations connected through LAN and share information in real time. Each station is responsible for a particular task thus making the size and cost of each station less than the one used in First Generation.

The network protocols used were still mostly proprietary, which led to significant security problems for any SCADA system that received attention from a hacker. Since the protocols were proprietary, very few people beyond the developers and hackers knew enough to determine how secure a SCADA installation was. Since both parties had vested interests in keeping security issues quiet, the security of a SCADA installation was often badly overestimated, if it was considered at all.

C. Third generation: Networked

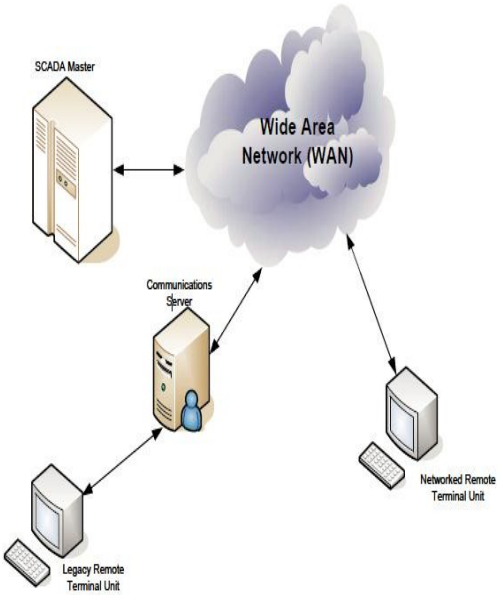


Fig 4: Third generation SCADA system[5]

Due to the usage of standard protocols and the fact that many networked SCADA systems are accessible from the Internet, the systems are potentially vulnerable to remote cyber-attacks. On the other hand, the usage of standard protocols and security techniques means that standard security improvements are applicable to the SCADA systems, assuming they receive timely maintenance and updates.

III. ATTACKS ON SCADA SYSTEM

An appropriate SCADA security strategy involves analysis of multiple layers of both the corporate network and SCADA architectures including firewalls, proxy servers, operating systems, application system

layers, communications, policies and procedures. Strategies for SCADA Security should complement the security measures implemented to keep the corporate network secure.

Successful attacks[9] can originate from either Internet paths through the corporate network to the SCADA network, or from internal attacks from within the corporate office. Alternatively, attacks can originate from within the SCADA network from either upstream (applications) or downstream (RTUs) paths.

An appropriate configuration for one installation may not be cost effective for another. Flexibility and the employment of an integrated and coordinated set of layers are critical in the design of a security approach network. Some of these and a brief description of their functions are as follows:

Border Router and Firewalls: Firewalls, properly configured and coordinated, can protect passwords, IP addresses, files and more. However, without a hardened

47 operating system, hackers can directly penetrate private internal networks or create a Denial of Service condition.

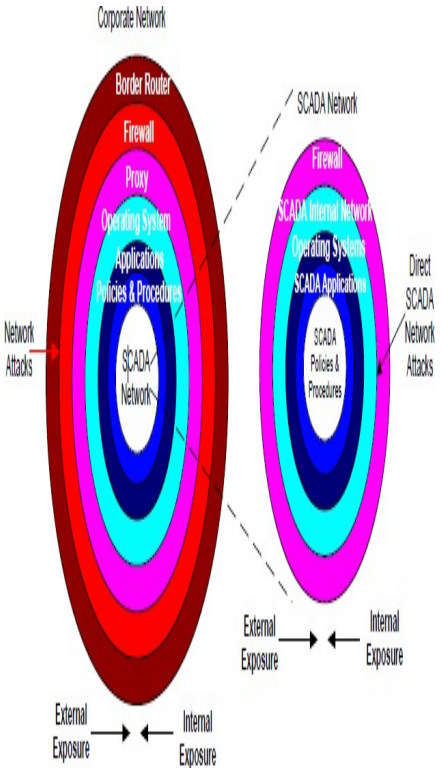
A. Proxy Servers: A Proxy server is an internet server that acts as a firewall, mediating traffic between a protected network and the internet. They are critical to re- create TCP/IP packets before passing them on, to, or from, application layer resources such as Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). However, the employment of proxy servers will not eliminate the threat of application layer attacks.

B. Operating Systems: Operating systems can be compromised, even with proper patching, to allow network entry as soon as the network is activated. This is due to the fact that operating systems are the core of every computer system and their design and operating characteristics are well known worldwide. As a result, operating systems are a prime target for hackers. Further, in- place operating system upgrades are less efficient and secure than design-level migration to new and improved operating systems.

C. Applications: Application layer attacks; i.e., buffer overruns, worms, Trojan Horse programs and malicious Active-X5 code, can incapacitate anti-virus software and bypass the firewall as if it wasn't even there.

D. Policies and Procedures: Policies and procedures constitute the foundation of security policy infrastructures. They include requiring users to select secure passwords that are not based on a dictionary word and contain at least one symbol, capital letter, and number, and should be over eight characters long. Users should not be allowed o use their spouse, child, or pet's name as their password. The above list is common to all entities that have corporate networks. SCADA systems for the most part coexist on the same corporate network [10]. The following list suggests ways to help protect the SCADA network in conjunction with the corporate network.

E. SCADA Firewalls: SCADA Systems and Industrial Automation Networks, like corporate network operating systems, can be compromised using similar hacking methods. Oftentimes, SCADA systems go down due to other internal software tools or employees who gain access into the SCADA systems, often without any intention to take down these systems. For these reasons, it is suggested that strong firewall protection to wall off your SCADA networking systems from both the internal corporate network and the Internet be implemented. This would provide at least two layers of firewalls between the SCADA networking systems and the Internet.



D. **Fig 5: Relationship between corporate and SCADA networks[10]**

IV. *SCADA Internal Network Design*: SCADA networks should be segmented off into their own IP segment using smart switches and proper sub-masking techniques to protect the Industrial Automation environment from the other network traffic, such as file and print commands. Facilities using Wireless Ethernet and Wired Equivalent Protocol (WEP) should change the default name of the Service Set Identifier6 (SSID)

V. PROPOSED METHOD

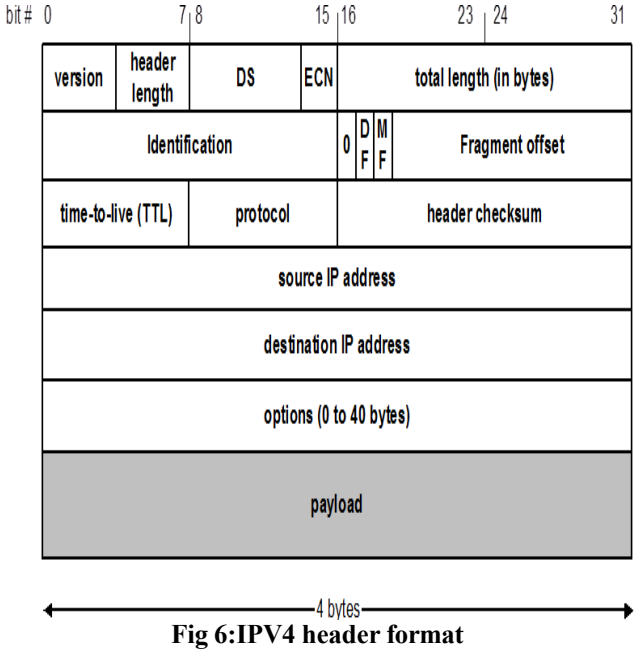


Fig 6:IPV4 header format

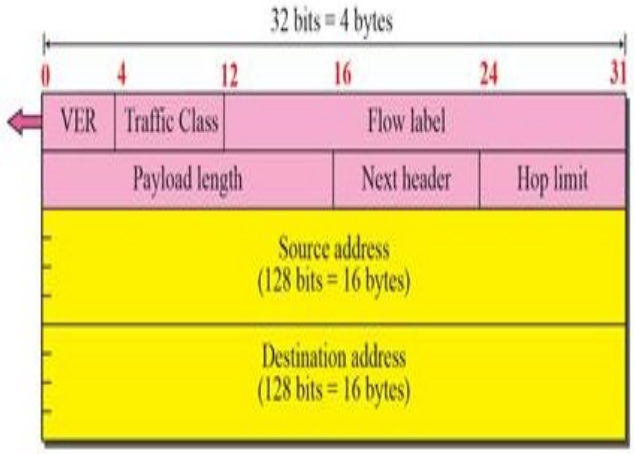


Fig 7:IPV6 header format

An efficient architecture has to be designed to prevent the different types of attacks on SCADA systems. In spite of the tremendous amount of security measures taken to prevent attacks on SCADA systems, the security of the SCADA systems has been compromised. To overcome these problems, in addition to the existing architecture, changes have to be made in the design of SCADA systems. The SCADA systems have to be designed with an additional firewall in their software and IPV6 capability as shown in figure 8.

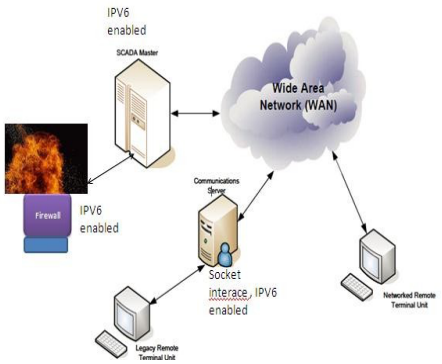


Fig 8: Proposed method for improved SCADA security.

The header format for IPV4 and IPV6 are shown in figure 6 and figure 7.The IPV6 has the features of extended addressing capability, header format simplification, improved support for extensions and options, flow label capability, authentication and lot of security features. The smooth transition from IPV4 to IPV6 can be done for all the platforms of operating systems by installing socket interfaces in the systems.These interfaces convert the IPV4 addresses to IPV6 addresses. The IPV6 address is a 128 bit address. The addresses are represented in hexadecimal format.

The different types of IPV6 addresses are unicast (can be global, link-local, site-local, unique local or IPV4 compatible), multicast (one-many), anycast (one-nearest) and reserved addresses. Link -local and site-local unicast addresses can be used during auto configuration and when no routers are present. Unique local IPV6 unique addresses have a global unique prefix with high probability of uniqueness and are intended for local communications and are not expected to be routable over the Internet. These addresses can be used when the SCADA systems are not required to be connected to the Internet. Even if they are accidentally leaked outside the site, they would not clash with any other addresses.

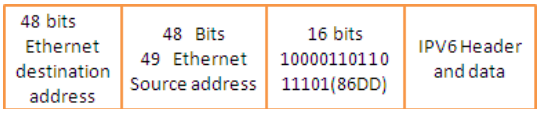


Fig 9: IPV6 addressing format

A variety of techniques can be implemented for transition to IPV6 like dual stack techniques to enable IPV4 and IPV6 to coexist in the same network and devices, tunneling techniques to avoid order dependencies when upgrading hosts, routers or regions and translation techniques to allow IPV6 only devices to communicate with IPV4 only

devices.

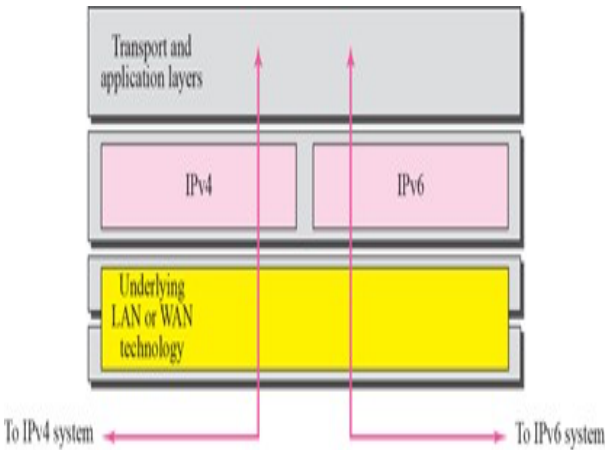


Fig 10: Dual stack method

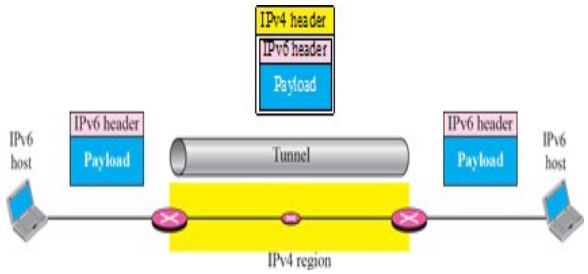


Fig 11: Tunneling strategy

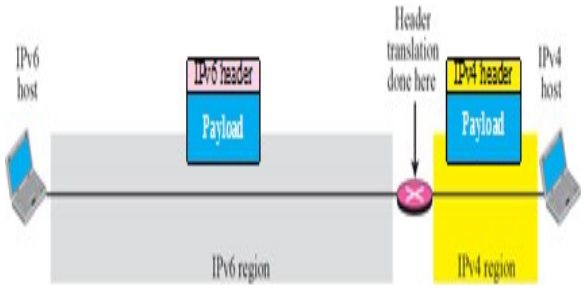


Fig 12: Header translation strategy

VI. Conclusion And Future Scope

The IPV4 addresses are at an exhaustion stage and this demands the necessity for transition to IPV6 addresses. The increased use of internet by billions of users across the world increases the problem of cyber security. The SCADA systems used in a multitude of applications are more prone to different types of attacks by hackers. The architecture of SCADA systems has to be modified in such a way that it can withstand the attacks and minimize data losses. The future of the Internet and SCADA systems relies on the ability to migrate to IPV6 and make the world a safer place less prone to attacks by hackers.

REFERENCES

[1] "Convergence Task Force Report," President's National Security Telecommunications Advisory Committee, Washington, DC, June 2001

[2] J. Walrand and P. Varaiya, High Performance Communication Networks, Second Edition, San Francisco: Morgan Kaufmann Publishers, 2000

[3] "Information Technology Progress Impact Task Force Report On Convergence," President's National Security Telecommunications Advisory Committee,Washington, DC, May 2000

[4] Walski, Thomas M., et. al., Advanced Water Distribution Modeling and Management, Haestad Press, January 2003

[5] McClanahan, R.H., The Benefits of Networked SCADA Systems Utilizing IPEnabled Networks, Rural Electric Power Conference, 2002. 2002 IEEE, 5-7 May 2002 Pages: C5 - C5_7

[6] IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation, IEEE Std 1379-2000 (Revision of IEEE Std 1379- 1997), 21 September 2000 [7]

Curtis, Ken, A., DNP3 Protocol Primer, DNP Users Group, 1 June 2000

[7] Marihart, D.J., Communications Technology Guidelines for EMS/SCADA Systems, Power Delivery, IEEE Transactions on,

[8] Volume: 16, Issue: 2, April 2001 Pages: 181–188

[9] "Critical Infrastructure Protection Challenges in Securing Control Systems", General Accounting Office (GAO) Report, GAO-04- 140T, October 1, 2003

[1] Pollet, Jonathan, SCADA Security Strategy, Plant Data Technologies, August 8, 2002