OVERVIEW OF WIRELESS NETWORK CONTROL PROTOCOL IN SMART PHONE DEVICES

P.L.Ramteke[1], D.N.Choudhary[2]

[1]Associate Professor, HVPM's College of Engineering & Technology, Amravati, Maharashtra State [INDIA]
[2]Professor & Head, Department of Information Technology, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, Maharashtra State [INDIA], ***[1]pl_ramteke@rediffmail.com, [2]dnchaudhari2007@rediffmail.com***

Abstract

The computer network connection without wire or any cable is referring as wireless network. These wireless local area networks are popular for its worldwide applications. It has covered wide scale wireless local area network. The large scale systems to all applicable areas make large numbers of wireless termination and covering very much area. To reduce the complexity associated with server management, Information Technology organizations begins the process of centralizing servers. It used with architecture principles of centralized management requirement for network to scale, network architecture needs to be able to support enhanced services in addition to just raw connectivity, distributed processing is required both for scalability ability and services, network support continuously increase the level of throughputs etc. Wireless LAN product architectures have evolved from single autonomous access points to systems, consisting of a centralized Access Controller and Wireless Termination Points.

The basic goal of centralized control architectures is to move access control, including user authentication and authorization, mobility & radio management, from one access point to centralized controller. The Wireless network Control Protocol allows for access and control of large-scale wireless local area networks. It can allows management of these networks, Control and Provisioning of Wireless Access Points In computer networking, a wireless access point is a device that allows wireless devices to connect to wired network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a router via a wired network, and can relay data between the wireless devices such as computers or printers and wired devices on the network

Keywords: *Wireless network control protocol, Wireless LAN, Wireless Transaction Protocol, Media Access Control*

----------*****----------

1. INTRODUCTION

Today wireless local area networks have great popularity but incompatible designs and solutions. C*ontrol and Provisioning of Wireless Access Points* is a standard, interoperable protocol that enables controller to manage a collection of wireless access points The Control and Provisioning of Wireless Access Points architecture taxonomy describes major variations of these designs. This protocol differentiates between data traffic and control traffic. The control messages are transmitted in a Datagram Transport Layer Security tunnel. The ability to interface with other devices using different wireless protocols could be used for remote sensing or instrument control. The camera can even potentially be used for direct data acquisition. Vodafone Wireless Innovation Project was compact

Microscopes that interface with a cell-phone camera. There is also nano sensor-based detector for airborne chemicals that plugs into an iPhone. Although envisioned for field use, these devices highlight the possibilities of the technology. Wireless Network Control Protocol recognizes the major architecture designs and presents common platform on which WLAN entities of different designs can be accommodated. This enables interoperability among wireless termination points and WLAN access controllers of distinct architecture designs. Therefore Wireless network Control Protocol allows for cost-effective wireless local area network expansions. It can also accommodate future developments in Wide LAN technologies. Figure 1 illustrates Wireless network Control Protocol operational structure in which distinct control elements are utilized for Local Media Access Control and Split MAC WTPs.

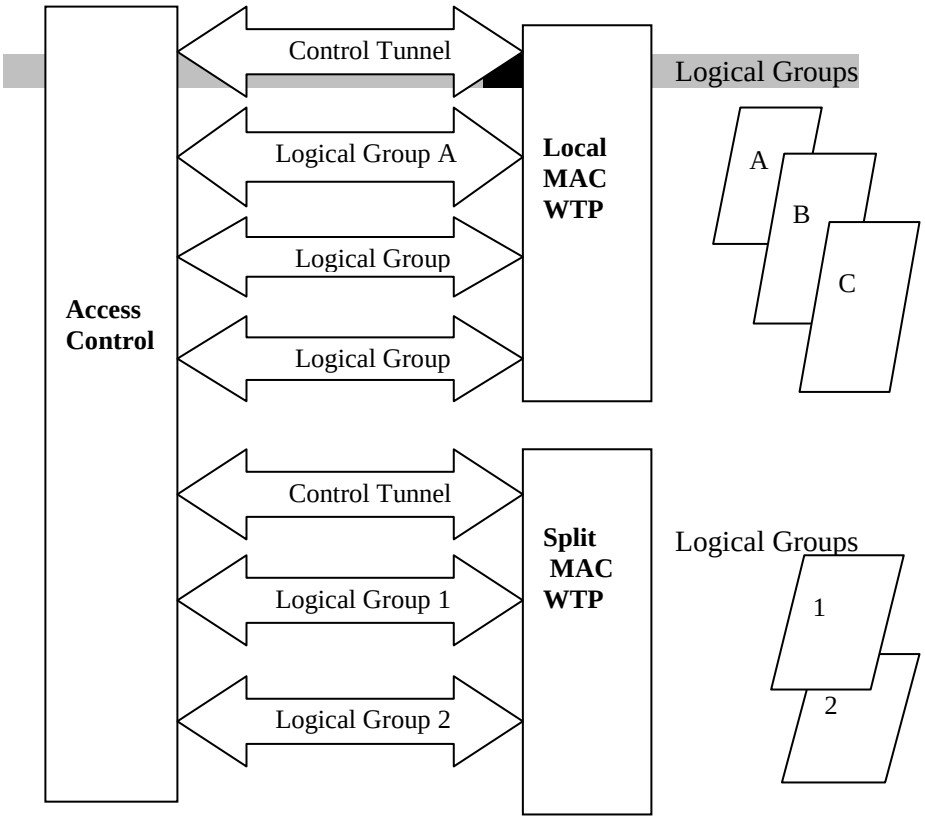

Figure 1 Wireless Local Area Network Control Protocol configuration

Wireless network Control Protocol also addresses the increasing trend of shared infrastructure. Its management needs to distinguish and isolate control for the different logical groups sharing single physical WLAN. WiCoP manages WLANs through a series of tunnels that separate traffic based on logical groups. The WiCoP operational structure is shown in Figure 1.Each WTP uses number of tunnels to distinguish and separate traffic for control and for each logical group. The protocol allows for managing WLANs in a manner consistent with the logical groups that share the physical infrastructure. Wireless network LAN Control Protocol operates control tunnels and logical group tunnels between the Access Control and two types of Media Access Control Wireless Termination Points. MAC is a unique identifier assigned to network interfaces for communications on the physical network segment. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model. MAC addresses are most often assigned by the manufacturer of a network interface card and are stored in its hardware, the card's read-only memory, or some other firmware mechanism. If assigned by the manufacturer, MAC address usually encodes the manufacturer's registered identification number. The control tunnels are used to transport messages dealing with configuration, monitoring, and management of Wireless Transaction Protocols. The logical group tunnels serve to separate traffic among each of logical groups constituting physical WTP.

2. PROTOCOL OVERVIEW

The Wireless network Control Protocol focuses on enabling interoperability in shared infrastructure WLANs. It is designed for use with different wireless technologies. The state machine for WiCoP is illustrated in Figure 2.

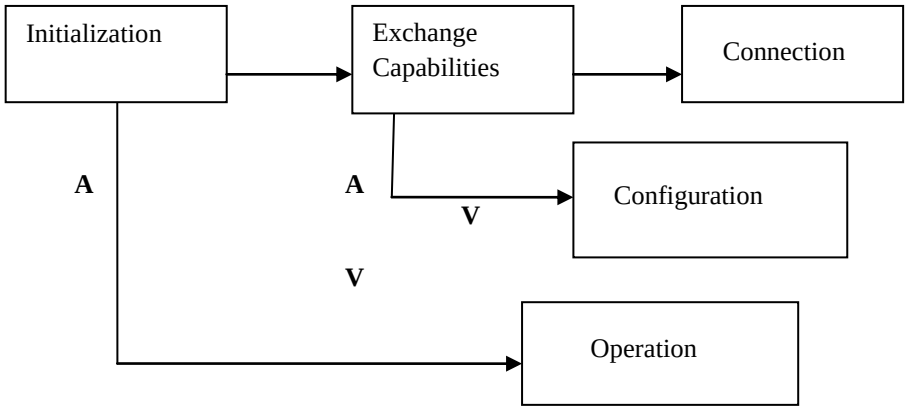

Fig.2 State machine for Wireless network control protocol

The Capabilities Exchange state represents initial protocol exchange between WTP and AC. In WTP state determines possible ACs from which it can receive management services. The Connection state represents the creation of a security infrastructure between a WTP and AC An AC in this state determines the capabilities of the WTP and the WTP's compatibility with management services. This involves mutual authentication and the establishment of secure connection between WiCoP entities. The Configuration state represents exchange of long-term operational parameters and settings between WTP and AC. A WTP in this state receives configuration information to operate consistently within WLAN managed by AC. An AC in this state provides configuration information to WTP based on the WTP's capabilities and network policies involved. The Operation state represents the active exchange of WiCoP monitoring and management messages. WTPs send regular status updates to and receive corresponding management instructions from the AC.This state involves firmware and configuration updates arising from changes in network conditions and administrative policies.WiCoP Format: Separate packets are used by WiCoP for control and data message transfer between AC and WTPs. A common header is used for both types of packets in which a single-bit flag distinguishes between them. WiCoP Header: Figure 3 illustrates the WiCoP common header for control and data packets.

```
 0          7          15          23          31
----|-------|-------|-------|-------|-------|----------
Version   |M|D|C|R|E|F|L| |          Reserve          |----------
----+-+-+-+-+-+-+-+-+-+---------------
 Fragment ID | Fragment No. |        Length          |----------
---+---------------+----------------------
```

Figure 3: Wi CoP Header Version Field

This field indicates the protocol version.'M' Field: The MAC-type field, 'M', distinguishes between Local MAC WTPs and Split MAC WTPs. It is used to efficiently realize interoperability between WTPs of the two different designs. A '0' value indicates WiCoP exchanges with Split MAC WTP while a '1' value indicates WiCoP exchanges with Local MAC WTP.

'D 'Field: the differentiator field,'D ', is used to distinguish between WTP variants within a type of WTP design. The CAPWAP Architecture illustrates that Split MAC design allows encryption/decryption to be performed at either the WTP or the AC. WiCoP acknowledges these major variants and accommodates them using 'D' field in MAC WTP, the 'D' field is used to indicate conjunction with the 'M' field. For a Split location of encryption/decryption while for a Local MAC WTP.

'C' Field: This field distinguishes between a WiCoP control and WiCoP data packet. Each type of information is tunneled separately across the WiCoP tunnel interfaces between WTPs and the AC. A '0' value for the 'C' field indicates a data packet; while a '1' value indicates a control packet. The 'C' field is also used to assign WiCoP packets to distinct data and control tunnels between the AC and WTP.

'R' Field: The retransmission field, 'R', is used to differentiate between first & subsequent transmissions of WiCoP packets. The 'R' field is used for critical WiCoP packets such as those relating to security key exchanges. A '0' value for the 'R' field indicates the first transmission of a WiCoP packet; while a '1' value indicates retransmission.

'E 'Field: the encryption field, 'E', is used to indicate if the WiCoP packet is encrypted between the AC and WTPs. The 'E' field is used for those WiCoP packets that are exchanged during initialization. A '0' value indicates the WiCoP packet is unencrypted, while a '1' value indicates the packet is encrypted.

'F' Field: The fragmentation field indicates if the packet is a fragment of larger packet. A '0' value indicates a non-fragmented packet while '1' value indicates a fragmented packet. The 'F', 'L', 'Fragment ID', and 'Fragment No.' fields are used together.

'L' Field: This field is used to indicate the last fragment of a larger packet. It is only valid when the 'F' field has a '1' value. A '0' value for the 'L' field indicates the last fragment of a larger packet while '1' value indicates an intermediate fragment of a larger packet.

Fragment ID Field: The Fragment ID identifies the larger packet that has been fragmented. It is used to distinguish between fragments of different large packets. This field is valid only when the 'F' field has '1' value. The 'F', 'L', 'Fragment ID', and 'Fragment No.' fields are used together.

Fragment No. Field: The fragment number field identifies the sequence of fragments of larger packet. The value of Fragment No. field is incremented for each fragment of larger packet so as to show the order of fragments. This field is valid only when the 'F' field has a '1' value. The 'F', 'L', 'Fragment ID', and 'Fragment No.' fields are used together.

3. WiCoP DATA PACKET

WiCoP data packets include the WiCoP common header followed by a payload. Data packets are used to distinguish traffic from control when both control and data paths are identical. Such scenario would involve data traffic of WTPs traversing the AC. However, given diversity of large-scale WLAN deployments, there are scenarios in which data and control paths are distinct. WiCoP can be used in both cases.

4. ACTIVE PRESENCE TIMER

The Active Presence Timer is used by each WiCoP entity AC and WTPs to verify the presence of each other. The absence of a reply to Feedback message within the expiration of the Active Presence Timer indicates the corresponding entity is inactive. Contingency operations such as reset are used in this case. The value of Active Presence Timer ranges from 10 to 300 seconds with a default value of 30 seconds.

5. WiCoP PROCESS

The processes of the Wireless LAN Control Protocol are described in this section with respect to the operational state in which they occur.

5.1. Initialization:

The Initialization state represents the initial conditions of WiCoP entities. WTPs and ACs in this state are powered on, run hardware self-check tests, and reset network interfaces. State transition: Initialization Capabilities Exchange WTP: Automatically upon detecting an active network interface AC: Upon receiving a Capabilities message from a WTP

5.2. Capabilities Exchange:

The Capabilities Exchange state allows WTPs to first find an AC and then to exchange capabilities information with it. WiCoP is designed to control WLANs with both Local MAC and Split MAC WTPs. The differences in their respective functional characteristics are determined in this state. The WTP first broadcasts Capabilities message as soon as it transitions from its Initialization state. The Capabilities message serves to discover ACs and contains information on its identity and capabilities. The AC receiving message transitions from its Initialization state. It examines compatibility with respect to the WTP type, its capabilities, and responds with an appropriate Capabilities Response message.

6. OPERATIONAL EFFICIENCY

The fact that WiCoP requires a single operation to distinguish and manage WTPs of different designs makes it operationally efficient. Because WiCoP assigns dedicated classification bits in the common header, an AC needs to parse incoming packets only once to determine particular manner in which it is to be processed. Without dedicated classifications in the common header, an AC would have to perform lookup after parsing every incoming packet, which would result in delaying processing. The scale and sensitivity of large- scale deployments require that WLAN control protocols be efficient in operation.

6.1. Semantic Efficiency: In certain cases, WiCoP combines utilities in a single operation. One particular case is that of statistics and activity feedback. Here, WTPs regularly send a single Feedback message containing statistics and other state information, which also acts as an implicit keep alive mechanism. This helps to reduce the number of message exchanges and also simplifies protocol implementation. Similarly, the Capabilities messages serve the purpose of finding ACs as well as informing them of WTP capabilities and design.

SUMMARY AND CONCLUSION

WiCoP includes trigger for suitable authentication mechanism. The Wireless LAN Control Protocol presents solution for managing large-scale WLANs with diverse elements. It addresses the challenges presented in CAPWAP Problem Statement and realizes the requirements of CAPWAP Objectives. WiCoP enables integral control of Split MAC and Local MAC WTPs by defining appropriate differentiators within the protocol message exchanges and processes. It

addresses architecture designs in which authenticator and encryption points are located on distinct entities. In doing so, WiCoP realizes the interoperability objective and its benefits. WiCoP also addresses shared WLAN deployments by configuring and managing WTPs on logical group basis. It is further provisioned to separate control and data traffic within WLANs. So, the protocol addresses the objectives of logical groups and traffic separation. Architecture designs in which authentication is performed at the AC and encryption at WTPs can be exposed to the threat of replay attacks.

ACKNOWLEDGEMENTS

The authors are thankful of researcher for their contribution in wireless networking and protocol who help and motivate us to contribute our work in this area.

REFERENCES

[1] Yang, L., Zerfos, P., and E. Sadot, "Architecture Taxonomy for Control and Provisioning of wireless Access Points (CAPWAP)", RFC 4118, June 2005.
[2] Govindan, S., Ed., Cheng, H., Yao, ZH., Zhou, WH., and L. Yang, "Objectives for Control and Provisioning of Wireless Access Points (CAPWAP)", RFC 4564, July 2006.
[3] O'Hara, B., Calhoun, P., and J. Kempf, "Configuration and Provisioning for Wireless Access Points (CAPWAP) Problem Statement", RFC 3990, February 2005.
[4]http://www.nature.com/nmeth/journal/v7/n2/full/nmeth0210-87.html
[5] Allman, M., Paxson, V. and W. Stevens, "TCP Congestion Control", RFC 2581, April 1999.
[6] Jacobson, V., Braden, R. "TCP Extensions for High Performance", RFC 1323, May 1992.
[7] Mathis, M., Mahdavi, J., Floyd, S. "TCP Selective Acknowledgment Options", , October 1996.
[8] Allman, M., Floyd, S. and C. Partridge, "Increasing TCP's Initial Window", October 2002.
[9] Dawkins, S., Montenegro, G., Kojo, M. and V. Magret, "End-to-end Performance Implications of Slow Links", BCP 48, RFC 3150, July 2001.
[10] Mogul, J. and S. Deering, "Path MTU Discovery", RFC 1191, November 1990.
[11] Knowles, S., "IESG Advice from Experience with Path MTU Discovery", RFC 1435, March 1993.
[12] McCann, J., Deering, S. and J. Mogul, "Path MTU Discovery for IP version ",August 1996.
[13] Ramakrishnan, K., Floyd, S. and D. Black, The Addition of Explicit Congestion notification (ECN) to IP", RFC 3168, September 2001.
[14] Allman, M., Balakrishnan, H. and S. Floyd, "Enhancing TCP's Loss Recovery Using Limited Transmit", RFC 3042, January 2001.
[15] Paxson, V. and M. Allman, "Computing TCP's Retransmission Timer", November 2000.
[16] Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., "RObust Header Compression Framework and four profiles:, July 2001.
[17] Degermark, M., Nordgren, B. and S. Pink, "IP Header Compression", RFC 2507, February 1999.
[18] Postel, J., "Transmission Control Protocol DARPA Internet Program Protocol Specification", STD 7, RFC 793, September 1981.
[19] Floyd, S. and T. Henderson, "The NewReno Modification to TCP's Fast Recovery Algorithm", April 1999.
[20] Bormann, C., "Robust Header Compression (ROHC) over PPP", RFC 3241, April 2002.

BIOGRAPHIES

P.L.Ramteke is working as a Associate Professor & Head at Information Technology Department. He is expertise in modeling and simulation, Mobile technology and software Engineering.

D.N.Choudhary is Professor & Heat at IT Departnet at JDIT's College of Engineering & Technology, Yavatmal.He is Ph.D. Supervisor & expert in Data Mining, Mobile Computing