IJCSET |August 2011 | Vol 1, Issue 7, 357-360

Improve the Performance of LBAC-IAPP by using Proactive Context Caching

Avayambal.K, T.Rajapuspha
Department Of CSE, MVJ College Of Enginerring, Bangalore-67

Abstarct: In wireless networks, continuous connectivity which allows user mobility and maintains the secured network utilization,is one of the most important requirements. WLANS are widely used in business, goverments, education and public. In order to establish wireless LAN with continuous connectivity, we need to employ additional mechanisms like IAPP, LBAC etc. In this paper, we used the concept of proactive context caching for LBAC-IAPP WLAN to provide continuous connectivity to secure wireless systems. In PCC the selected neighbouring base stations exchange link quality information of the mobile node through distributed system and the information stored in to the cache memory of mobile stations.Based on the quality information the LBAC directional IAPP WLAN the connectivity will be maintained between different access points. It reduces interuption time, handoff delay complexity.

Keywords: LBAC (Location based Access control), IAPP (Inter access point protocol), WLAN, PCC (Proactive Context switching), RADIUS (Authentication server)

I.INTRODUCTION:

In recent years IEEE 802.11 [4][5] and mobile devices such as cell phones, PDA and smart cards are widely used due to ease of connection. Many places for example universities, companies, airport, shopping malls provide wirelesss LAN services to attract the customers. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks:

- Mobility-Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- Installation Speed and Simplicity-Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Reduced Cost-of-Ownership-While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, ads, and changes.
- Scalability-Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that allows roaming over a broad area.

The 802.11 standards allow the realization of economic wireless LANs that support data rates anywhere from 1Mbps to 54Mbps based on the distance to the access point. So in future WLAN will be available anytime and anywhere (4G Wi- Fi). The challenging issues for the WLAN is identified in following categories

i) Transcations are broadcasted over the air (Security attacks remote Authentication scehemes are not suitable for mobile devices)
ii) Connectivity with the access points while roaming (Hand-off delay)
iii) Limited bandwidth and computational power
iv) Interoperability with Wired Infra -structure.

The users of IEEE 802.1x[5] need to enter the passsword inorder to access the network. So there is a need to employ additional mechanisms to protect the communications which the users can easily setup and access in WLAN to provide a continuous connectivity. Recently a lot of research activities have been initiated to provide easy reassociation while roaming.

In this paper we use Proactive Context Caching for location based access control called LBAC –IAPP [1].This procedure uses IEEE 802.11f called IAPP [6] to transfer context information.

The rest of the paper is organized as follows. Section II provides an overview of LBAC- IAPP. Section III describes the proactive context caching to improve the performance. Section IV describes conclusion and ended with references.

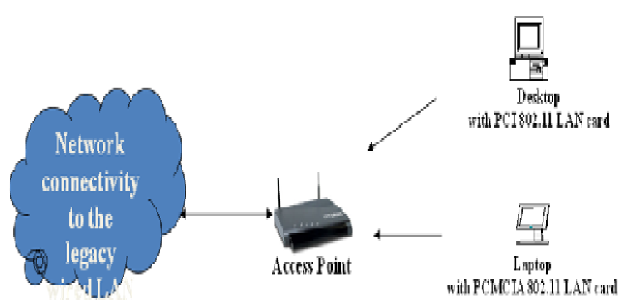

Fig 1. Overview of Wireless LAN (IEEE 802.11)

II. OVERVIEW OF LBAC AND IAPP

A. IEEE 802.11 :

Fig 1 describes the components of Wireless LAN. IEEE 802.11 [4] provides network connectivity over wireless media. An Access Point (AP) is installed to act as Bridge between Wireless and Wired Network. The AP is connected to wire network and is equipped with antenna to provide wireless connectivity. The range (Distance between Access Point and WLAN client) depends on structural hindrances and RF gain of the antenna at the Access Point. To service larger areas, multiple APs may be installed with a 20-30% overlap. A client is always associated with one AP and when the client moves closer to another AP, it associates with the new AP (Hand-Off). WLAN are available in three flavors 1. 802.11b 2. 802.11a 3.802.11g

B. IEEE 802.11f : IAPP (Inter Access Point Protocol)

IAPP [6] (Inter Access-Point Protocol) is designed for the enforcement of unique association throughout an ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period. Based on security level, communication session keys between APs are distributed by a RADIUS server. The IAPP is implemented on top of IP and is an extension to existing management protocols.

Association: The IAPP entity must be able to find and use a RADIUS server to look up the IP addresses of other APsin the ESS. When the given BSSIDs of those other APs (if a local capability to perform such a translation is not present) used to obtain security information to protect the content of certain IAPP packets (By RADIUS Client). Fig 2(a) describes phenomena of association.

Reassociation: IAPP relies on a STA making use of ReassociationRequest frame when roaming from one AP to another, in order to provide the most complete services to the APs. When a STA uses the 802.11 Association Request, rather than the Reassociation Request, the IAPP may not be able to notify the AP at which the STA was previously associated of the new association.Fig 2(b) describes the complete phenomena about reassociation with different APs of Wireless LANs.

C. Location Based Access Control.(LBAC):

The LBAC-IAPP [1] architecture shown in Figure includes the three elements, mobile nodes (Ss), access points (APs) and a RADIUS (Authentication server). The LABC-IAPP Mechanism can be divided into four Phases.

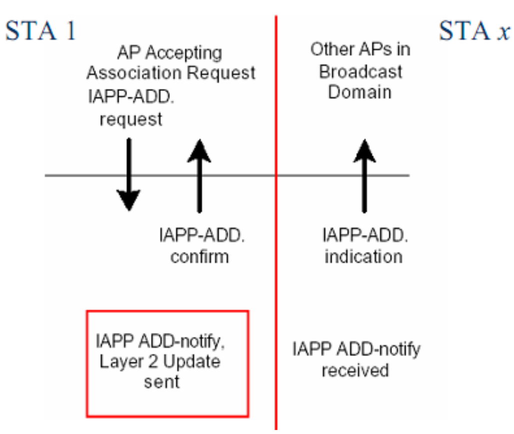

Fig2 (a). IAPP protocol Overview (Association)

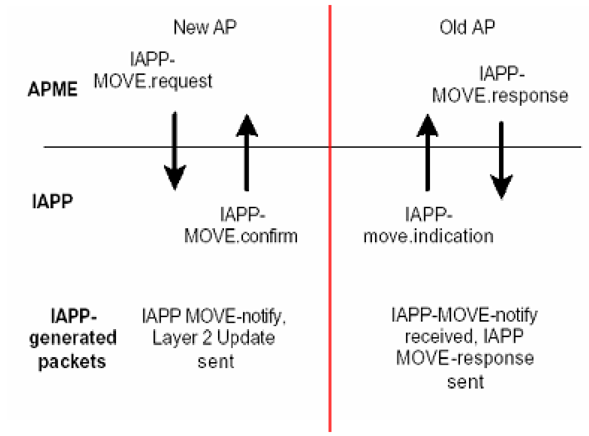

Fig2 (b) . IAPP protocol Overview (reassociation)

(1)Discovery phase: When the mobile node is located within the access granted-area defined by the location group G_L= {AP1, AP2, AP3}, the mobile node will send a probe request to each channel in the location group. After APs receiving this frame, the APs record context information about the MAC address and timeout of mobile node in the LBAC-IAPP table.

(2)Authentication Phase: After receiving the probe request, APs sends an IAPP-AUTHINFO.request to other APs in location group through the authentication server, in order to verify whether the APs have received the probe request from the mobile node.

(3)Acknowledgement Phase: When other APs receive AUTHINFO.request. The APs will reply an IAPP-AUTHINFO.response to that the sending AP through authentication
server to acknowledge status of discovery from mobile node in location group.

(4)Connection Phase: After the AP acknowledged status of mobile node through IAPP-AUTHINFO.response signal, the AP will inspect the existence of mobile node from other APs in location group. And if the mobile node exists in location group, the AP will allow the mobile node to access the authentication process based on IEEE 802.11 standard.
Fig 4 shows the overview of LBAC- IAPP, in this figure operation steps are marked by number, and message flows are indicated by arrows.

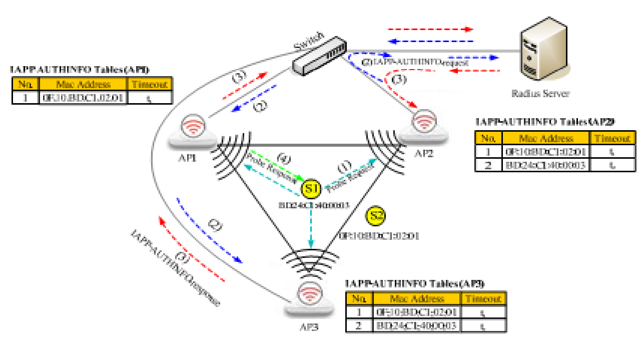

Fig 4. Overview of LBAC-IAPP

III. PROACTIVE CONTEXT CACHING:

This paper presents the PCC with LBAC-IAPP in WLAN systems. In this section we propose a PCC algorithm to improve the connectivity in LBAC directional propagation.
PCC [2] includes the following three sections:

1)Neighbor Graphs & Dynamic Learning
First a neighbor graph [3] is constructed at each AP in a distributed fashion and the MH's context is propagated to all neighbor APs and it will be stored in the local caches of AP based on the neighbor group. The neighbor graph represents the handoff probability from a given AP to each neighbor AP. Based on the neighbor information; the MH context is propagated only to the selected AP's. Cache entries are dynamically updated with its neighbor information.

2) Proactive cache algorithm:
The LBAC-IAPP [1] architecture shown in Fig.8 includes mobile node (MN), Access points (AP). When the mobile node is located with in the access granted area defined by the location group G_L={AP1,AP2,AP3}. PCC [2][6] uses the following frame format defined in Fig 5 , 6, 7 and Table 1 to maintain the caches in AP.

IAPP Version	Command	Identifier	Length	Data
Octets: 1	1	2	2	0-n

Fig 5.Frame format for IAPP

Table 1.The command values

Value	Command
0	ADD-notify
1	MOVE-notify
2	MOVE-response
3	Send-Security-Block
4	ACK-Security-Block
5	CACHE-notify
6	CACHE-response
~~5~~7-255	Reserved

Address Length	Reserved	MAC Address	Sequence Number	Current AP	Context Length	Length of Context Block	Context Timeout
Octets: 1	1	n = Address Length	2	n	2	m = Length of Context Block	2

Fig 6:Format for CACHE-NOTIFY

Address Length	Status	MAC Address	Sequence Number
Octets: 1	1	n = Address Length	2

Fig 7: Format for CACHE RESPONSE

This algorithm can be divided in to four steps..
Case (i): Mobile node is in current AP.

- If cache is having the data then Probagate
- Cache entry is not there send the request to the RADIUS and get CACHE NOTIFY from RADIUs.

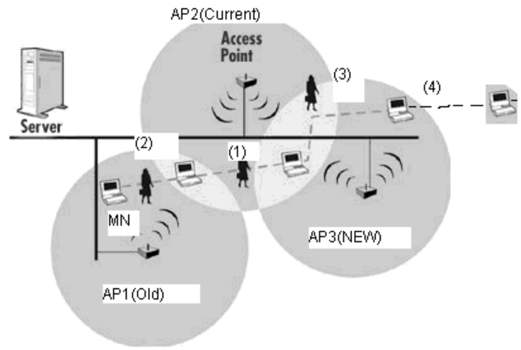

Fig 8. Description about working principle of PCC

Case (ii): Mobile node is moving form old AP to current AP.

- If cache is having the data then Probagate
- Cache entry is not there send the request to the RADIUS and get CACHE NOTIFY (Fig 6) from RADIUS and send CACHE RESPONSE (Fig 7) to the RADIUS.
- Cache entry is refreshed from old AP by using replacement algorithm.

Case (iii): MN is moving from cueerent AP to the new AP **(**Reassoaciation)

- If cache is having the data then Probagate
- Cache entry is not there, send the request to the RADIUS and get CACHE NOTIFY from RADIUS.
- Cache entry to be updated in new AP Based on neighbor graph.

Case (iv): MN is moving to non neighbor AP.

- Dynamically the caches of non neighbor AP will be updated with a use of RADIUS by old, current or new AP's.So hand-off wont affected during the reassociation in LBAC-IAPP.

3) Consistency caching
Cache pages are frequently refreshed by using LRU replacement algorithm.

IV. CONCLUSION

We proposed a PCC for LBAC-IAPP. In this PCC we described the CACHE NOTIFY & CACHE RESPONSE to avoid the disruption time of LBAC directional propagations at different angles mentioned in [1].LBAC-IAPP eliminates the dependence on Global Positioning System(GPS) and it provides the minimum computational overhead and complexity. This is the one of the promising techniques for network access control based n/w on WLANS for public, government and shopping malls etc.
To evaluate the proposed algorithm we are on the process of simulating the PCC on NCTUNS 6.0.

REFERENCES

[1] Tanatat Saelim Prawit Chumchu – "ICOIN 2011" A New Algorithm for Location-Based Access Control Using IAPP in WLANs

[2] Teck Chaw Ling, Jen Funn Lee, Kian Pee Hoh2 - Malaysian Journal of Computer Science, Vol. 23(1), 2010 - Reducing Handoff Delay In Wlan Using Selective Proactive Contextcaching

[3] SangheonPacka HakyungJunga TaekyoungKwona YangheeChoi A-Mobile Computing and Communications Review, Volume1, Number2 : SNC:A Selective Neighbor Caching Schemefor Fast Handoff in IEEE802.11WirelessNetworks

[4] http://www.pulsewan.com/

[5] http://www.networkworld. com/ aboutus /index.html

[6] Inter Access Point Protocol (IAPP) 802.11fComputer Network laboratory