K.Swetha / International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 4, pp.1303-1305

A Review on Fast Handoff Mechanism in Mobile Adhoc Networks Using CSA-PHMIPv6

K.Swetha

ABSTRACT- In this paper, PHMIPv6 proposes to select the node with the highest signal strength as the partner node. and CSA- PHMIPv6 for which mobile hosts select partners with whom communication can last for a sufficiently long time by employing the Link Expiration Time (LET) parameter.

INDEX TERMS- Mobile IP, MIPv6, HMIPv6, PHMIPv6, mobility management and mobile networks.

I.Introduction

The internet-based applications have transformed the mobile networks into all IP configuration frameworks. IP does not support mobility. Mobile IP is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address[1]. Mobile IPv6 faces the problem of long delays and high packet losses during a handoff.

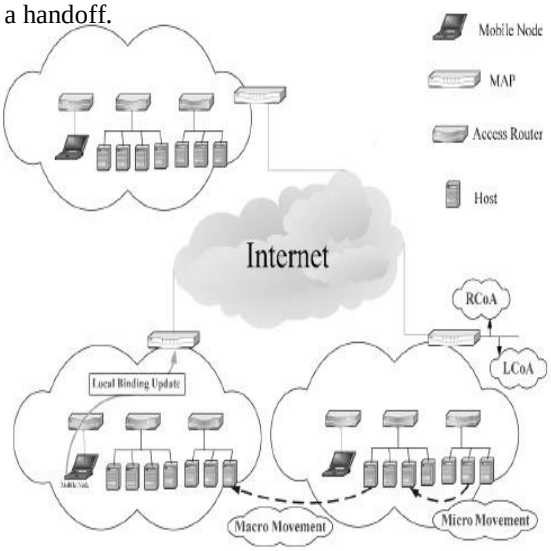

Fig 1. HMIPv6

HMIPv6 protocol is designed to minimize the amount of signaling to correspondent(s) and to the home agent by allowing the mobile node to locally register in a domain[9]. It has been proposed to provide a method for efficient mobility management in a network, where mobile nodes frequently change their access routers.
HMIPv6 may result in loss of packets and service disruptions undermining the QoS, when mobile node moves at a high speed or overlaps between two adjacent access points.
To overcome this, PHMIPv6 has been introduced, mobile host choose partners based on their signal strength. However, depending on its speed, it is easily possible that the PN with the strongest signal may fade away from the mobile host or the new Access Point before the handoff operation is finalized. In addition to the cost associated with the gratuitous exchange of signaling messages between the MH and PN, this will get the mobile host back to the former situation where it has to initialize the handoff by itself.

II. Partner based Hierarchial Mobile IPv6

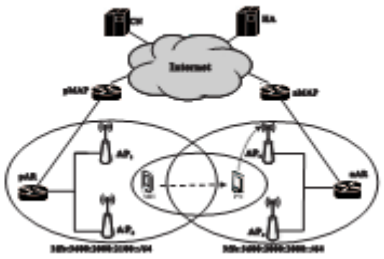

Fig 2. PHMIPv6 System Architecture

This is based on HMIPv6 protocol [4] which is denoted as Partner-based HMIPv6 (or PHMIPv6) protocol. Our PHMIPv6 protocol utilizes a PN to improve the handoff latency during the handoff process.The PN is a mobile node which is located with the MN in different MAP domain and can directly communicate with the MN by the using ad hoc network[3]. The main task of PN is to perform the pre-handoff procedure for the MN before MN

reach to a new MAP domain. The other functions of the PN are the same as the MN.

The PHMIPv6 protocol divides the network into two IPv6 subnet domains. MH sends the data packets from the AP and previous AR to the CN through the previous MAP. That is, CN sends data packets to the RCoA of MH, and MAP then forward the packets to the LCoA of MH. While MH moves into a new MAP domain, MH performs the registration procedure to its nMAP. The macro-mobility is occurred if MH switches from a pMAP to a nMAP domain. Then, MH must acquires a new unique CoA to register the CoA to new access router and nMAP. Observe that, in our PHMIPv6 protocol, MH performs the registration procedure with the assistance of PN if PN is existed during the macro-mobility.

Since the original PHMIPv6 selects unknown PNs for performing handoff operations, it is vulnerable to the following security threats. Adequate security measures should be incorporated in the enhanced version of PHMIPv6 so that these security risks are carefully addressed and dealt with[7].

Malicious PN: First, a MH provides its corresponding PN with its security key for Authentication, Authorization, and Accounting (AAA) purposes in the original PHMIPv6 scheme. This security key can be reused at a later time by a malicious PN, to bind with the access point posing itself as the MH. This may be of particular benefit to the PN in case that this security key provides the PN with a higher service level than what it is originally entitled for. We take this security flaw into account in our enhancements to the PHMIPv6 scheme by allotting two different security keys to the PN and the MH for pre-handoff request and authentication with the wireless network operator/service provider, respectively.

Malicious MH: The second security risk is pertaining to a malicious MH, which aims at flooding the access point/router with multiple pre-handoff requests and eventually causes a Denial of Service (DoS)[5]. To this end, the malicious MH may send pre-handoff requests to a large number of PNs concurrently. In our envisioned enhancement to the original PHMIPv6 scheme, this threat can be addressed by permitting only one pre-handoff request for every MH, which can be easily identified by its unique security key.

A. Connection Stability Aware PHMIPv6

PHMIPv6 selects the node with the highest signal strength as the partner node. and CSA- PHMIPv6 for which mobile hosts select partners with whom communication can last for a sufficiently long time by employing the Link Expiration Time (LET) parameter.

To address this issue, we propose the use of Link Expiration Time (LET) [6] as a parameter in the selection of the best possible PN, which will be able to communicate with the new AP for a sufficiently long time.

Although the use of GPS should become commonplace in mobile nodes, we introduce a scheme to estimate the LET without the need of GPS. We use the Doppler shift subjected to packets to calculate the relative velocity of nodes. The distance between nodes is calculated using the scheme used in [10], which uses the power of signals to calculate the distance between the nodes by using the simplified free space propagation model given in [2]. For the mobility model it is assumed that mobile nodes are pseudo-linear, and highly mobile in nature. A good example of this kind of system is an aeronautical ad hoc network [8].

III. CONCLUSION

In this paper, the proposed approach takes into account the nodes' dynamicity in terms of the Link Expiration Time used to carry out the cooperative handoff by maintaining stability of the connections between a MH, its respective PN, and other involved entities. In addition, incorporate security features to circumvent malicious threats against the mobile hosts and/or the partner nodes. Efficient adoption of cooperative diversity based communications through the proposed approach may indeed prove quite useful to roaming nodes in ad hoc wireless networks.

REFERENCES

[1] T. S. Rappaport, Wireless Communications: Principles and Practice, Prentice Hall, 1996.

[2] H. Soliman, C. Catelluccia, K. El Malki, and L. Bellier, *"*Hierarchical mobile IPv6 mobility management (HMIPv6)*"*, Network Working Group, RFC 4140, Aug. 2005.

[3] Y. S. Chen, W. H. Hsiao, and K. L. Chiu, *"*Cross-Layer Partner-Based Fast Handoff Mechanism for IEEE 802.11 Wireless Networks*"*, in Proc. IEEE VTC, Baltimore, USA, Sep. 2007.

[4] E. Sakhaee, T. Taleb, A. Jamalipour, N. Kato, and Y. Nemoto, *"*A Novel Scheme to Reduce Control Overhead and Increase Link Duration in Highly Mobile Ad Hoc Networks*",* in Proc. IEEE WCNC, Hong Kong, China, Mar. 2007.

[5] Tarik Taleb,Zubair Md.Fadlullah,Marcus Scholler and Khaled Ben Letaief,"A connection Stability Aware Handoff Management Scheme" in wirelessand Mobile Computing,2009,IEEE International Conference.

[6] Y. S. Chen, W. H. Chuang and C. K. Chen, *"*DeuceScan: Deuce-Based Fast Handoff Scheme in IEEE 802.11 Wireless Networks*",* in IEEE TVT, Vol. 57, No. 2, Mar. 2008, pp. 1126-1141.

[7] I. Ramani and S. Savage, *"*SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks*",* in Proc. IEEE Infocom, Miami, Florida, USA, Mar.2005.

[8] S. Pack, H. Jung, T. Kwon, and Y. Choi, *"*A Selective Neighbor Cashing Scheme for Fast Handoff in IEEE 802.11 Wireless Networks*",* in Proc. IEEE ICC, Seoul, South Korea, May 2005.

[9] W. K. Lai and J. C. Chiu, *"*Improving Handoff Performance in Wireless Overlay Networks by Switching Between Two-Layer IPv6 and One-Layer IPv6 Addressing*",* IEEE JSAC, Vol. 23, No. 1, Nov. 2005. pp. 621-628.

[10] D. Kim, C. K. Toh, J. C. Cano, and P. Manzoni, "A bounding algorithm for the broadcast storm problem in mobile ad hoc networks," in Proc. IEEE Wireless Communication and Networking Conference, WCNC'03, vol. 2, pp. 1131-1136, New Orleans, LA, USA, Mar. 2003.