Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 722 – 728

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

A Fast Handoff Technique in Wireless Mesh Network (FHT for WMN)

Geetanjali Rathee[a], Hemraj Saini[b]

[a,b]*Department of Computer Science & Engineering*
Jaypee University of Information Technology, Waknaghat-173234 INDIA

Abstract

In dynamic nature of WMN, handoff latency is a significant parameter of research. When a mesh client leaves the range of serving mesh router and searches for accessing a new router based on good SNR (Signal to Noise) ratio, a handoff procedure takes place. Whenever a mobile client leaves the range of its Home Mesh Router (HMR) and connects to a Foreign Mesh Router (FMR), mobile (roaming) client needs to authenticate itself as a legitimate node to its FMR in order to get the network services. Several handoff authentication techniques have been suggested by different researchers but leads to certain types of drawbacks i.e. handoff latency, computational overhead, security threats and storage overhead. In order to overwhelm over these hitches, this manuscript propose a technique Fast Handoff Technique (FHT). The suggested technique is compared and evaluated over the network metrics i.e. handoff latency and computational overhead. Further the approach is proved by describing a formal analysis over parameters.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Handoff; WMN; FHT; Authentication.

1. Introduction

Wireless Mesh Network (WMN) is a new cohort network that has occurred recently. It is a mishmash of ad-hoc and mesh networks[1]. Due to dynamic nature of WMN[2, 3], handoff delay[4] is one of the current topic of research. In general, handoff is defined as the movement of a client from one router's range to another routers range (as depicted in figure 1). During mobility, as the distance between client and its (Home Mesh Router) HMR increases, mobile clients need to search for a new mesh router in order to get the fast network services. The Foreign Mesh Router

Corresponding author. Tel.+91- 9736248186;
E-mail address: geetanjali.rathee123@gmail.com.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.095

(FMR) is selected on the basis of good signal strength between roaming client and mesh router. Whenever a roaming client connects to FMR, it needs to authenticate itself to it for accessing the network services. During handoff authentication process, there exist a delay between the request send by a roaming client to authenticate itself and the time it gets authenticated to its FMR. A significant time to authenticate a roaming client with its FMR causes a latency in network which may cause several threats inside the network i.e. communication overhead, computation overhead and security threats. In order to get rid over these problems, different researchers have proposed several handoff authentication techniques. The next section discussed some previously proposed approaches with their limitations.

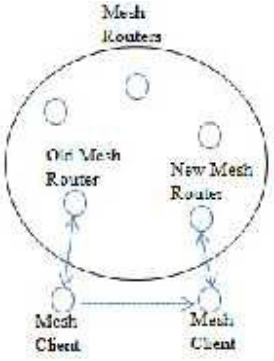

Fig. 1. Wireless Mesh Network Architecture

2. Related Works

In order to access the services, roaming client needs to authenticate with FMR. Handoff latency is defined as the time taken by the client to authenticate itself after moving from its range to another routers range. To reduce handoff latency in multi-hop WMN[5], researchers have proposed various schemes which are basically divided into two types. i) public key based; where user and authenticator authenticates each other without contribution of third party and ii) symmetric key based; in which security is recognized with the involvement of third party. The below text discusses some handoff authentication techniques.

Anmin et al.[6] proposed a security context transfer scheme in which latency is reduced through security context keying parameters and materials. In this scheme, a dynamic user sends a Context Transfer Activation Request (CTAR) to new access mesh router; meanwhile previously accessing mesh router directs CTAR message to new mesh router that provisions authorization token (as shown in fig. 2). New mesh router compute token using parameters provided by foregoing mesh router and compare it with one confined in context activation request.

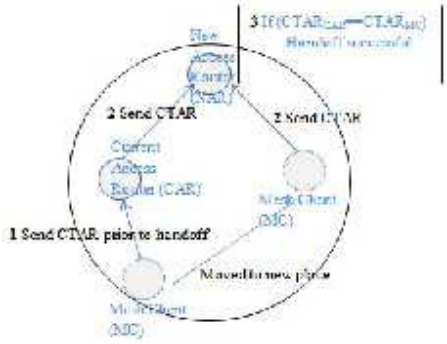

Fig. 2. (a) CTAR Scheme

The major drawback with this parameter is the latency during token sent by old mesh router to Foreign mesh Router. C. M. Huang[7] proposed a cluster chain mechanism in order to fast the handoff process but limitation with this is that an extra trust relationship is required between every duos of neighbor authenticator which marks trust model intricate. Further the trust between the routers are maintained by SLAB[8] technique through local authentication but this approach is also suffers from one extra drawback i.e. computational overhead along with latency. The techniques discussed by Li Xi and Paul[9, 10] are able to reduce the above limitations but encountered with security attacks. Xi Li proposed a ticket based authentication where an authentication server is responsible for generating the tickets. Server distributes all the tickets independently to individual mesh router and mesh clients but as all the data is stored at mesh clients that may cause a threat of several types of security attacks. The number of handoff mechanism schemes with their cons is describing in table 1. Although the researchers are able to reduce handoff latency but still there exist some other drawbacks (i.e. computational and communication overhead, storage overhead and security threats[11]) that needs to be considered. So, there is a need to propose a technique which is resilient against above limitations.

Table 1. Simulation Parameters.

Protocol	Technique	Drawback
CTAR[6]	Security Context	Computational Overhead
CCCT[7]	Cluster-chain Transfer Scheme based on context mechanism	Additional trust relationship between every pair of neighboring nodes
SLAB[8]	Synchronization of LHAP updating at Mesh Router	Communication overhead, handoff latency
THA[9-10]	Ticket based Handoff	Storage Overhead

2.1. Manuscript Contribution

In this manuscript, a fast handoff authentication technique is offered which takes less computation and communication overhead. The proposed approach reduces the handoff latency by generating the tickets for handoff authentication. The technique is proved by comparing the latency parameter with CTAR scheme and computational overhead with THA technique.

The structure of the paper is systematized as follows. Section two deliberates the proposed technique to reduce handoff latency. Further section three and four debates the performance and formal analysis of the technique. Finally section five concludes the paper.

3. Proposed System

The abbreviations of the proposed technique that are going to be used throughout the manuscript are shown in table 2.

Table 2. Abbreviations Meaning

Abbreviations	Meaning
AS	Authentication Server
HMR	Home Mesh Router
FMR	Foreign Mesh Router
MC	Mesh Client
GMK	Group Master Key
MK	Master Key
Ti	Ticket

In proposed technique, a number of symmetric encryption keys are generated between communicating parties (i.e. server-Mesh Client, server-Mesh Routers, Mesh Routers-Mesh Clients) for authentication. Further server generates the tickets based upon the keys generated between server and mesh client. The detailed explanation of the proposed scheme is described in further text. The proposed model of the technique is depicted in fig. 3.

3.1. Proposed Technique Steps

After generating the keys between each other, Foreign Mesh Router FMRi validate roaming mesh client by matching the ticket Ti. Previous servicing mesh router sends ticket Ti to foreign mesh router upon receiving the handoff request from roaming mesh client. As the roaming client show its ticket Ti to FMR upon request for handoff authentication. FMRi checks the validity of client and makes the hand off successful, if Ti sent by roaming client matches with the Ti sent by previous servicing mesh router. The key generation and key distribution process of proposed technique is depicted in fig. 4. The depicted figure shows a server who is responsible for generating the tickets and the keys between mesh clients and mesh routers. The stepwise description of the approach is explained below.

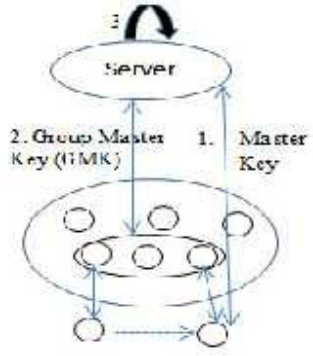

Fig. 3. Proposed Model

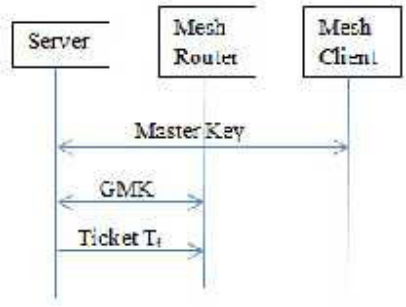

Fig. 4. Key and Ticket Generation Process

- Initially, a MK generates between the server and MC for mutual authentication.
- Further, Selected mesh routers generates a group based master key GMK between AS-MR and this single GMK will be used by all mesh routers.
- AS will generate ticket Ti for corresponding ID's of mesh routers based on GMK and distribute tickets to all the routers.
- Whenever a MC moves from HMR to FMR, roaming client will ask for corresponding ticket from AS and shows the ticket to FMR.

If (Ticket client==Ticket HMR) **then**
Handoff verification successful
Else
Handoff Authentication Fails

The algorithm corresponding to the proposed approach is depicted in table 3.

4. Performance Evaluation

We have analyzed the proposed technique by comparing it with two different handoff authentication techniques i.e. Ticket Handoff Authentication (THA for short) [10] and secure Context Transfer Protocol (CTAR for short) [6]. Further, in order to prove the efficiency of proposed technique FHT, it is evaluated over certain parameters i.e. handoff latency and computational overhead on ns2 simulator. The parameters of simulation are shown in Table 4.

The simulation is done over NS2 simulator where numbers of nodes are taken as 250. The area size is fixed as 400*400 with a MAC of 802.11. The traffic source is constant bit rate having 512 bytes.

Table 3. Proposed Algorithm

Input: Roaming MCi wants to authenticate itself to its FMRi **Output**: MCi Roaming client may get the network services after authenticate itself with less handoff latency and communication overhead to the FMRi.
Key generation process 1. Master key is generated between server and an individual mesh clients 2. A group of mesh routers are responsible to generate a group based master key GMK between server and mesh routers.

Authentication Process
1. Server generates the tickets for all the mesh clients corresponding to their mesh routers.
2. Tickets are distributed independently to each mesh client and mesh router by the server
3. During authentication phase, mesh router will ask a ticket Ti from roaming mesh client Ci.
If (Ticket client == ticket HMR) **then**
Handoff authentication successful and client may get the services
Else
An attack is encountered and Handoff authentication fails

Handoff latency and computational overhead are the two significant parameters to be measured during handoff. A significant delay to prove the authenticity of roaming client with its mesh router may cause several security threats i.e. user privacy, denial of service attack and black hole attack.

Table 4. Simulation Value

Parameters	Size
No. of nodes	250
Area Size	400*400
MAC	802.11
Simulation Time	30 sec
Traffic source	CBR
Packet Size	512 bytes
Antenna	Omni Antenna

Further a large computational time between roaming mesh client and authentication server may cause different types of performance degradation i.e. storage overhead, network load, traffic congestion and deadlock in the network. So, in this manuscript the proposed approach is measured against the techniques THA (for short) through computational overhead and handoff latency through CTAR scheme. Further the approach is proved by discussing some formal analysis.

4.1. Handoff Latency

The suggested approach is equated with CTAR technique and analyzed in terms of handoff latency parameter. The below graph fig. 5 shows handoff latency comparison. In our proposed technique FHT, Server pre-distributes the tickets to mesh routers before handoff procedure which reduces latency during handoff. Whenever a roaming client comes under the range of FMR, foreign mesh router authenticates roaming client by requesting its ticket and validates the client if ticket stored in routers database matches with the ticket sent by the client. While in case of CTAR scheme, FMR request the ticket of corresponding roaming client with the old mesh router which may cause a significant delay and leads to handoff latency.

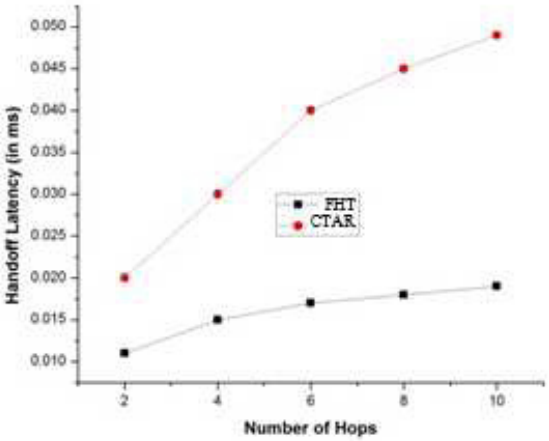

Fig. 5. Handoff Latency Graph

4.2. Computational Overhead

Computational Overhead is measured in terms of time required to compute master key between AS-MR and corresponding tickets Ti generation time. Because of lesser number of keys management and generation, computation overhead at proposed technique is much less as compared to THA as depicted in fig. 6. Because in proposed technique group based master key is generated among mesh routers. A single key is shared amongst all the routers which may reduce the management process at server side as well as at client side.

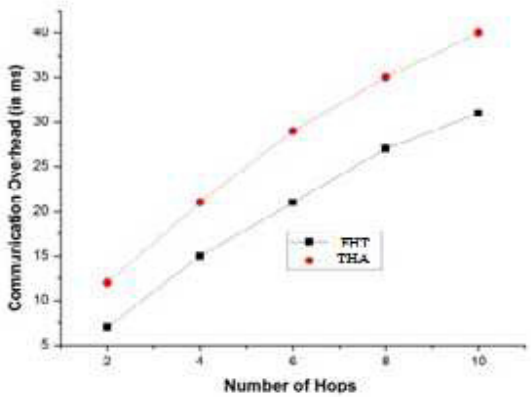

Fig. 6. Computational Overhead Graph

5. Formal Analysis

Computational overhead and handoff latency are the two significant parameters which are analyzed through NS2 simulator. Now, to prove the efficiency of proposed technique, a formal analysis is done over two more parameters i.e. key management overhead and ticket storage load. Below text gives a brief discussion of FHT on these two parameters.

5.1. Key Management Overhead

An individual master key MK is shared between each MC-AS while a multicast session key is used to generate the keys between AS-MR. A single GMK is used among all the mesh routers which reduces the key management and storage overhead at both AS and mesh routers database.

5.2. Ticket Storage Load

Mesh routers need to store their own tickets in spite of storing all router tickets and the roaming mesh client requests for ticket Ti to AS only during handoff authentication. So, storage overhead of tickets at mesh routers is negligible while at mesh clients it is none.

6. Conclusion

In order to fasten the handoff procedure, an efficient technique is proposed called FHT which is able to reduce handoff latency and computational overhead in significant manner. Further a formal analysis is done on the approach which is able to reduce key management and ticket storage overheads. The FHT technique is proved by showing the proper simulation results on NS2 simulator and discusses formal analysis.

References

1. Akyildiz, Ian F., and Xudong Wang.A survey on wireless mesh networks. In; *IEEE conference on Communications Magazine*, 43(9), 2005.
2. A. A. Franklin and C. S. R. Murthy. An introduction to wireless mesh networks. *Security in Wireless Mesh Networks(book chapter), CRC Press*,USA;2007.
3. Ben Salem, N. & Hubaux, J.-P.:Securing Wireless Mesh Networks. In:, *IEEE Wireless Communication*, 13(2), pp. 50-55, 2006,.
4. Amir, Yair, et al. Fast handoff for seamless wireless mesh networks.*Proceedings of the 4th international conference on Mobile systems, applications and services*. ACM, 2006.
5. Draves, Richard, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. *Proceedings of the 10th annual international conference on Mobile computing and networking*. ACM, 2004.
6. J. Loughney, M. Nakhjiri, C. Perkins, R. Koodli, Context transfer protocol (CXTP), 2005.
7. C.M. Huang, J.-W. Li, A cluster-chain-based context transfer mechanism for fast basic service set transition in the centralized wireless LAN architecture, Wirel. Commun. Mobile Comput. 9, pp. 1387–1401, 2009.
8. H. Zhu, X. Lin, R. Lu, P.-H. Ho, X. Shen, SLAB: a secure localized authentication and billing scheme for wireless mesh networks, IEEE Trans. Wirel. Commun. 7, pp. 3858–3868, 2008.
9. A. Fu, Y. Zhang, Z. Zhu, X. Liu, A fast handover authentication mechanism based on ticket for IEEE 802.16m, IEEE Commun. Lett. 14 , pp. 1134–1136, 2010,.
10. Xu, Li, et al. "Ticket-based handoff authentication for wireless mesh networks." Computer Networks 73 , pp. 185-194, 2014.
11. Goransson, Paul, and Raymond Greenlaw. Secure roaming in 802.11 networks. Newnes, 2011.