Efficient Handoff Routing (EHR) in WMN

Geetanjali Rathee
Department of Computer Science and Engineering
Jaypee University of Information Technology
Waknaghat-173234, INDIA

Hemraj Saini
Department of Computer Science and Engineering
Jaypee University of Information Technology
Waknaghat-173234, INDIA

ABSTRACT
In WMN, handoff is a significant parameter of research. Whenever 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. During mobility, packet transmission may enhance the number of security threats and network performance degradation issues which needs a secure routing protocol to be considered. In order to overwhelm over these hitches, this manuscript proposes a technique called Efficient Handoff Routing EHR. The suggested technique is compared and evaluated over network metrics i.e. handoff latency, throughput, end-to-end delay and packet delivery ratio. Further the approach is proved by describing a formal analysis over parameters.

Keywords
Handoff, routing, security, EHR,WMN.

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 where the clients may directly communicate with each other and forward the data packets to their destination nodes [1]. Due to broadcasting and dynamic nature of WMN [2, 3], handoff latency [4] plays an important role and is one of the current topic of research. In general, handoff is defined as the movement of a client from one routers range to another routers range (as depicted in fig. 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 (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 for accessing the network services or if a roaming client wants to send some messages to another client, it needs to select some secure routing algorithms in order to secure the data packets from several attacks. During mobility, routing packets can be easily forged by an attacker and can do some unethical changes during packet transmission. In handoff routing process, a number of possible threats exist to degrade the network performance i.e. end-to-end delay, throughput, latency and packet delivery ratio. A significant time to route the data packets causes latency in the network which may cause several threats inside the network with other parameter degradations i.e. end-to-end delay 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.

2. RELATED WORK
In order to access the services, roaming client needs to authenticate with its FMR. Further if a mobile client wants to send some data packets to another client; mobile client needs to send its data packet through some routing algorithm for their packet security. During 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. Further several security algorithms have been proposed by different researchers but these algorithms cannot adopt well during mobility. The below text discusses some handoff and secure routing techniques.

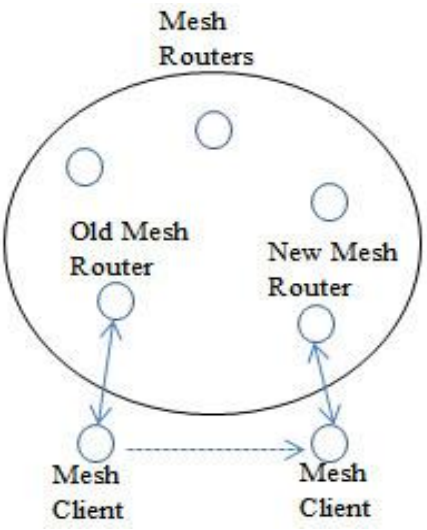

Fig 1: Handoff in WMN

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 the CTAR message to new mesh router that provisions authorization token (as shown in fig. 2). Further new mesh router compute token using parameters provided by foregoing mesh router and compare it with one confined in context activation request. The major drawback with this parameter is the latency during token sent by old mesh router to Foreign mesh Router.During mobility, whenever a client wants to send some data packets, different number of attacks can be performed by several attackers i.e. performance degradation, security broadcast etc. A number of researchers have performed several secure routing techniques.

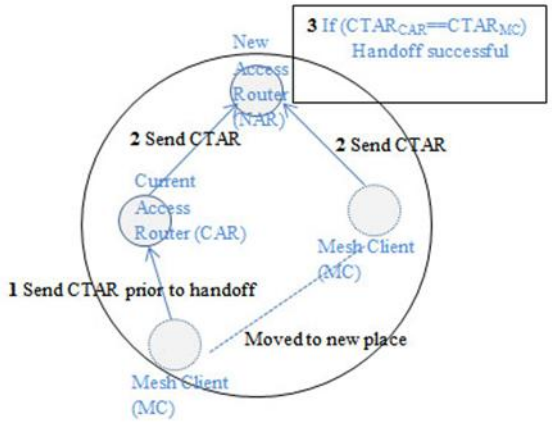

Fig 2: CTAR Schemes

SAODV [7] is a secure routing protocol which secures the data packets using digital signatures and hash chains. Digital signatures are used to secure the packets while hash chains secure the counting hops of routes. Although the hop count in routing can be reduced but attackers may attack the routing table of each node. Further FPBPKD [8] another secure routing protocol uses a proactive key distribution mechanism to cope up against corrupted transit access points but encounters with certain backbone layer attacks. Further 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 [11,12]. The number of handoff mechanism and secure routing schemes with their cons is describing in table 1. Although the researchers are able to reduce handoff latency and security issues but still there exist some other drawbacks (i.e. computational and communication overhead, storage overhead and security threats) that needs to be considered [13, 14]. So, there is a need to propose a technique which is resilient against above limitations.

Table 1. Related Work

Protocol	Technique	Drawback
CTAR	Security Context	Computational Overhead
CCCT	Cluster-chain Transfer Scheme based on context mechanism	Additional trust relationship between every pair of neighboring nodes
THA	Ticket based Handoff	Storage Overhead
SAODV	Hash chains and digital signatures	Enhances the security risks by involving third party broker
FPBPKD	4-way handshake proactive key distribution	Security issues exits in the backbone network

2.1 Manuscript Contribution

In this manuscript, an efficient handoff routing technique is offered which takes less handoff latency and increase the network performance by increasing the security level with Packet Delivery Ratio and Throughput. The proposed approach reduces the handoff latency by generating the tickets for handoff authentication and secures the routing packets by using diffie Hellman key exchange algorithm. Further the efficiency is increased through bellman ford algorithm to find the shortest path to route the packets. The technique is proved by comparing the latency parameter with CTAR scheme and end to end delay, packet delivery ratio and throughput against SAODV protocol.

3. PROPOSED APPROACH

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
RC	Roaming Client
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. In this,server generates the tickets based upon the keys generated between server and mesh client. Further bellman ford [15] and diffie Hellman key exchange algorithm [16] are used to route and secure the data packets.The detailed explanation of the proposed scheme is described in further text. The proposed model of the technique is depicted in fig. 3. The suggested approach is divided among certain subsections as discussed in below texts.

3.1 Key Generation and Authentication Verification Process

The key and ticket generation process for authenticating the roaming mesh client is depicted in fig. 3 where a master key is generated between server and a mesh client while a group based master key is created among mesh routers and servers. A ticket Ti is generated by an Authentication Server AS containing the source address, destination address and a time stamp T used to authenticate the mobile client during initial transmission. After successful authentication verification of a roaming client, it may access and perform any operation inside FMRi.

3.2 Secure Routing Process

After successful authentication verification, whenever a roaming client wants to send some data packets to another client within a single domain, then to enhance the routing process and securely transmit the data packets to destination node, bellman ford algorithm and diffie Hellman key exchange techniques are used.

Bellman ford algorithm is used to find the shortest path between communicating nodes to enhance the network parameters i.e. end-to-end delay, PDR and throughput. Further during packet transmission, a number of attacks can be performed by different attackers to alter or modify the routing packets. To prevent from these hitches, diffie Hellman

key exchange algorithm is used to encrypt the data packets during routing so that even if the packet is forged, it cannot be seen by an attacker or easily altered by the attacker.

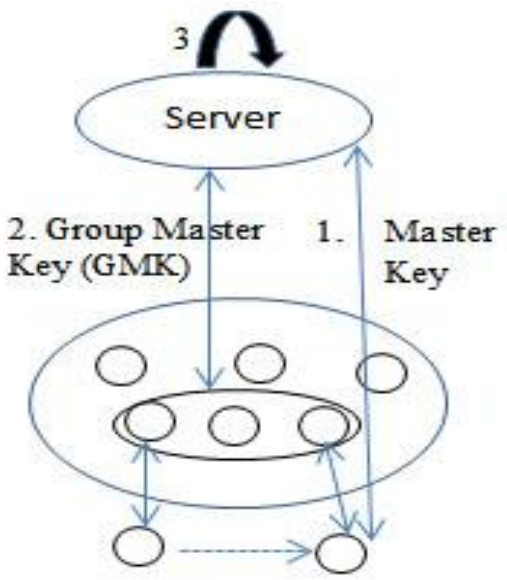

Fig 3: Proposed Model

The below text deliberated the above discussion through various steps.

- Initially, a master key MK is engendered 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 among all mesh routers to reduce the key management overhead.
- Authentication Server AS will generate ticket Ti for corresponding ID's of mesh routers based on GMK and distribute the tickets to all the routers.
- Whenever a MC moves from HMR to FMR, roaming client will ask for corresponding ticket of that roaming client from AS and shows the ticket to FMR

If ($Ticket_{client}$==$Ticket_{HMR}$) then

1. Handoff verification successful and roaming client is able to do the communication and access the certain network services.
2. **If** (roaming client RCi wants to communicate the data packets) then

a. Source code S will find the shortest path to the destination using bellman ford algorithm.

b. After selecting the shortest path, Diffie Hellman key exchange algorithm is used to encrypt the data packets.

End if

End if

Else

Handoff Authentication Fails and roaming client is not able to access any network services.

End Else

The algorithm corresponding to the proposed approach of handoff and secure packet transmission is depicted in table 3.

Table 3. Proposed Algorithm

Input: Roaming client MCi wants to access the network services with FMR domain and transfer some messages with the client within that domain.

Output: Roaming client MCi may get the network services after authenticating itself with less handoff latency and securely transmit the messages within FMR domain.

Key generation process

1. A Master key is generated between server and individual mesh clients.
2. In order to reduce key generation and management overhead, a group of mesh routers are responsible to generate a group based master key GMK between server and mesh routers.

Authentication and Secure Routing Process

1. Authentication Server AS 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 during authentication verification process.
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 network services

If (RC wants to communicate with another client Ci) **then**

A shortest path will be chosen among source and destination using bellman ford algorithm and transmit the data packets by encrypting with diffie Hellman key exchange algorithm.

End If

End If

Else

An attack is encountered

Handoff authentication fails and client is not able to get the network services.

End Else

To prove the integrity of the proposed work, proper simulation results are shown by considering various performance factors.

4. PERFORMANCE EVALUATION

The proposed technique is analyzed over two different techniques i.e. Ticket Handoff Authentication (THA for short) [10] for handoff latency and other network parameters i.e.end to end delay, throughput, packet delivery ratio with SAODV technique [6]. Further, in order to prove the efficiency of proposed technique EHR, it is evaluated over above mentioned parameters on ns2 simulator. The parameters of

simulation environments 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.

Handoff latency, throughput, end-to-end delay and packet delivery ratio are the significant parameters to be measured during handoff routing.The reason for selecting these parameters are that 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, black hole attack.

Further the data packets during mobility may enhance the security threats as well as performance degradation issues.

Table 5 shows the simulation values of network parameters of both existing and proposed approach.

Table 4. Simulation Parameters

Parameters	**Size**
Number of Nodes	250
Area Size	400*400
MAC	802.11
Simulation Time	30 sec
Traffic Source	CBR
Packet Size	512 bytes
Antenna	Omni Antenna

The below subsections discussed various simulating parameters with their discussions.

Table 5. Simulation Values

Simulation Parameters with their Approaches		**Different Network Size**			
Network Parameters	**Approach**	10	20	30	40
Handoff Latency (in ms)	Basic Approach	10	14	16	18
	Proposed Approach	20	23	25	27
End to End Delay (in ms)	Basic Approach	150	210	300	380
	Proposed Approach	90	120	180	210
Packet Delivery Ratio (in %)	Basic Approach	95	87	79	71
	Proposed Approach	97	93	89	83
Throughput (in %)	Basic Approach	97	94	91	89
	Proposed Approach	99	97	94	92

4.1 Handoff Latency

The suggested approach is equated with CTAR technique and analyzed in terms of handoff latency parameter. The below graph fig. 4 shows handoff latency comparison. In our proposed technique EHR, 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.

4.2 End to End Delay

It is measured as the time required to generate the packets by the source and packet reaches to its destination node. The formula of end to end delay is given in equation 1.

$$End\ to\ End\ Delay = \frac{Packets\ \ generated\ \ by\ Source}{Packets\ \ reac hes\ to\ destination} \qquad (1)$$

The proposed technique used bellman ford algorithm to transmit the data packets through shortest path and securely transfers the message using diffie Hellman key exchange algorithm. The depicted fig. 5 shows the end to delay graph of proposed and existing approaches.

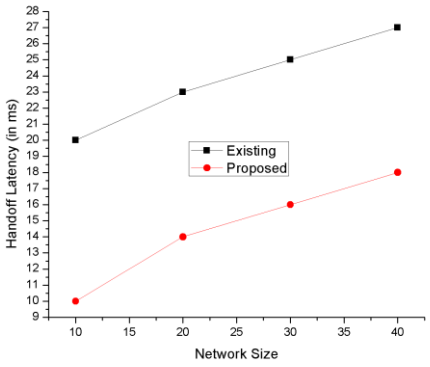

Fig 4: Handoff Latency Graph

4.3 Packet Delivery Ratio (PDR)

PDR is defined as the number of packets reaches to destination node divided by number of packets transmitted by source node. The formula of Packet Delivery Ratio (PDR) is given in equation 2.

As seen from depicted fig. 6, PDR of proposed approach is better than existing because of encrypting the data packets using diffie Hellman. The attackers may not see or alter the data packets transmitted by the source node.

$$PDR = \frac{packet\ \ reac hes\ at\ destination\ \ node}{packet\ \ generated\ \ by\ sou rce\ node} \qquad (2)$$

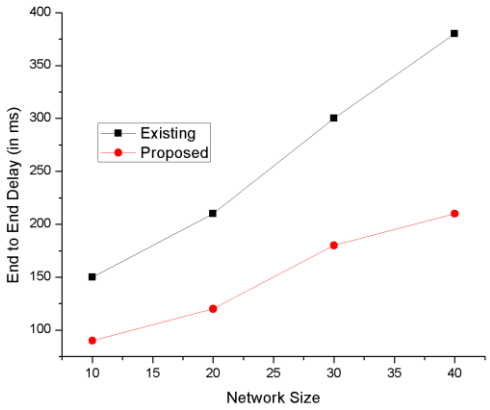

Fig 5: End to End Delay

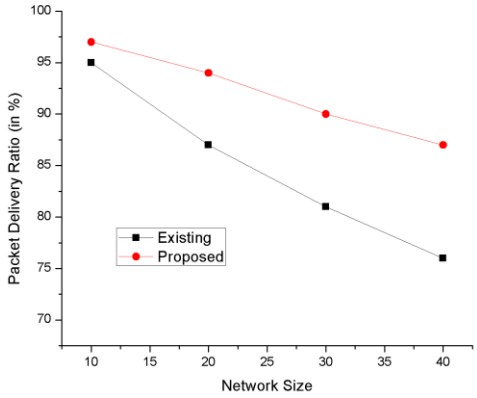

Fig 6: Packet Delivery Ratio

4.4 Throughput

The secure packet transmission and shortest route to transmit the data packets is the major reason of throughput enhancement in proposed approach. The depicted fig. 7 shows the throughput graph in comparison of proposed and existing approach.

To strengthen the proposed task, a formal analysis is also discussed over certain parameter in next section.

5. FORMAL ANALYSIS

Security attacks, overhead and handoff latency are the significant parameters which are analyzed through NS2 simulator. Now, to prove the efficiency of proposed technique, a formal analysis is done over certain parameters i.e. key management overhead, ticket storage load, attack resistant, and efficiency. Below text gives a brief discussion of EHR on these 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 recycled among all the mesh routers which reduces the key management and storage overhead at both AS and mesh routers database.

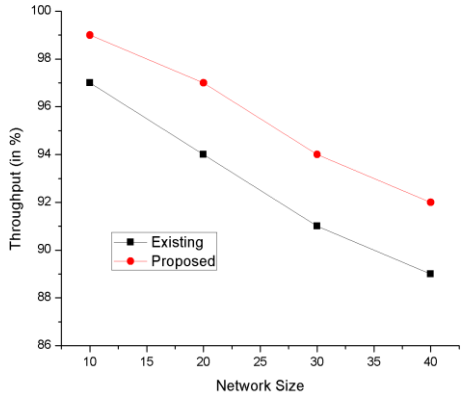

Fig 7: Throughput

5.2 Ticket Storage Overhead

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.

5.3 Attack Resistant

Each client transmits the data packets by encrypting with the keys generated via Diffie Hellman key exchange algorithm. So, packets cannot be seen during routing inside the network and even if the messages are forged by an attacker, it is in encrypted form and cannot be interpret by the intruder.

5.4 Efficiency

The proposed protocol is more efficient as it uses the bellman ford algorithm to find the shortest path and route the data packets through this path. Another advantage of shortest route selection is that, it may fasten the transmission process to the destination node.

6. CONCLUSION

In order to enhance the security level during mobility, a proficient routing technique i.e. Efficient Handoff Routing (EHR) is proposed. The proposed approach uses ticket generation and key exchange mechanism to securely transmit the data packets with minimum delay. The technique is analyzed over ns2 simulator which securely conveys the data packets with minimum end to end delay and handoff latency. Further EHR technique is proved by discussing a formal analysis over attack resistant, ticket storage and key management overhead and parameters.

The future scope of this paper is to test the proposed approach on a test bed and analyze the results in real time environment.

7. REFERENCES

[1] Akyildiz, I. F., Xudong W.A survey on wireless mesh networks. 2005. In; IEEE conference on Communications Magazine, 43(9).

[2] Franklin A.A., Murthy C. S. R.2007. An introduction to wireless mesh networks. Security in Wireless Mesh Networks(book chapter), CRC Press,USA.

[3] Ben Salem, N., Hubaux, J.-P. 2006. Securing Wireless Mesh Networks. In: IEEE Wireless Communication, 13(2), pp. 50-55.

[4] Amir, Yair,.2006. Fast handoff for seamless wireless mesh networks.Proceedings of the 4th international conference on Mobile systems, applications and services. ACM.

[5] Draves, R., Jitendra P., Brian Z. 2004. Routing in multi-radio, multi-hop wireless mesh networks. Proceedings of the 10th annual international conference on Mobile computing and networking. ACM.

[6] Loughney, L., Nakhjiri. M., Perkins .C.,Koodli. R. 2005. Context transfer protocol (CXTP).

[7] Lu S, Li L, Lam K Y, Jia L. 2009. SAODV: a MANET routing protocol that can withstand black hole attack, In:IEEE International Conference on Computational Intelligence, pp. 421-425.

[8] Kassab M, Belghith A, Bonnin J, Sassi S. 2005. Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks, In: Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling, pp 46-53.

[9] Fu,A., Zhang, Y., Zhu ,Z., Liu , X. 2010. A fast handover authentication mechanism based on ticket for IEEE 802.16m, IEEE Communication. Letter. 14, pp. 1134–1136.

[10] Xu, Li. 2014. Ticket-based handoff authentication for wireless mesh networks." Computer Networks 73 , pp. 185-194.

[11] Hill, D.W. and Lynn, J.T., Motorola, Inc., 2000. Adaptive system and method for responding to computer network security attacks. U.S. Patent 6,088,804.

[12] Simmonds, A., Sandilands, P. and Van Ekert, L., 2004. An ontology for network security attacks. In Applied Computing (pp. 317-323). Springer Berlin Heidelberg.

[13] Bansal, M., Rajput, R. and Gupta, G., 1999. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. The internet society.

[14] Huang, P., Feldmann, A. and Willinger, W., 2001, November. A non-instrusive, wavelet-based approach to detecting network performance problems. In Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. pp. 213-227. ACM.

[15] Cheng, C., Riley, R., Kumar, S.P. and Garcia-Luna-Aceves, J.J., 1989, August. A loop-free extended Bellman-Ford routing protocol without bouncing effect. In ACM SIGCOMM Computer Communication Review Vol. 19, No. 4, pp. 224-236. ACM.

[16] Bresson, E., Chevassut, O. and Pointcheval, D., 2001. Provably authenticated group Diffie-Hellman key exchange—the dynamic case. In Advances in Cryptology—ASIACRYPT 2001. pp. 290-309. Springer Berlin Heidelberg.