University of Cincinnati

Date: 3/4/2010

I, Saugat Joshi, hereby submit this original work as part of the requirements for the degree of Master of Science in Computer Science.

It is entitled:
Fast and Efficient Mutual Authentication in Wireless Mesh Networks (WMNs)

Student's name:  Saugat Joshi

This work and its defense approved by:

Committee chair:  Dharma Agrawal, DSc
Committee member:  Raj Bhatnagar, PhD
Committee member:  Yizong Cheng, PhD
Fast and Efficient Mutual authentication in Wireless mesh Networks (WMNs)

A thesis submitted to the

faculty of the University of Cincinnati

In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

In the Department of Computer Science

Of the College of Engineering and Applied Science

March 4, 2011

by

Saugat Joshi

B. E. (Electronics and Communications)

KLS’s Gogte Institute of Technology

Visvesvaraya Technological University, Belgaum, India

Thesis Advisor and Committee Chair: Dr. Dharma P. Agrawal
Abstract

Through the evolvement of high speed internet, Wireless mesh networks (WMNs) have become one of the most exciting and promising technology for providing high bandwidth features to its users. Along with the advancement of internet, the demand for enhanced capacity and higher bandwidth requirement have strived over time to meet the requirements of the Quality of Service (QoS) in WMNs. Various factors do affect the desired Qos for WMNs. In this thesis, we focus on the key generation scheme for authentication between various entities of the network to establish a secure communication between them, while taking into consideration the QoS requirements set by the benchmark. The key generation scheme discussed here is decentralized and hierarchal in nature which enables a pair of entity (e.g., servers and clients) to share a common key for a secure communication. Moreover, the scheme addresses the issue of the high speed mobility of the clients stations (STAs) from one domain to another domain, i.e. handoff between various inter- domain and intra- domain Access Points (APs). It is necessary that the STAs do not require excessive overhead during the handoff procedure. The schemes discussed enables faster and secure key generation and agreement scheme between the entities of the network during the handoff procedure.

The key generation scheme is distributed in nature. The higher level hierarchy namely the Internet Gateways (IGWs) or the authentication, authorization and accounting (AAA) servers such as RADIUS, generate a multi variate symmetric polynomial function and exchange the information among them such that none of them have a complete knowledge of the entire generated function. As the functions are passed to the lower level hierarchical entities such as Mesh access points (MAPs), the function further reduces providing only legitimate information to them. The process continues until the lowest level of the hierarchy (STAs or clients) is reached where the entities will be able to deduce a secure key for the communication. We refer to this as a distributed mechanism or a distributed authenticated key establishment (AKE) scheme based on hierarchical multi-variable symmetric functions (HMSF). Since, the deduced key is obtained from distributed scheme and below various levels none of the entities have a complete knowledge to reverse engineer the original function used in the generation process. Using the distributed authenticated key establishment scheme the STAs and MAPs could authenticate among themselves without any assistance from the higher hierarchy entities, thus saving the communication overhead time and the delay involved in authentication by getting back to the servers hence maintaining the required QoS.
Acknowledgments

I would like to heartily thank Dr. Dharma P. Agrawal for his continuous support and motivation for the completion of my thesis. From the scratch to the final results his inputs have played a vital role in the thesis. I would also like to thank Dr. Raj Bhatnagar and Dr. Yizong Cheng, for being in my committee. Further, I would like to express my thanks to Dr. Bing He for helping me set up the simulation environment, validate the results and for the continuous feedback. Moreover, I would like express thanks to all my colleagues in Center of Distributed Mobile and Computing (CDMC). Finally, I would like to thank my parents and grandparents for their support and belief in me without which this would not have been possible.
# Contents

1. Introduction .......................... 9
   1.1 Wireless Mesh Networks ................................................................. 9
   1.2 Application of wireless mesh networks .............................................. 11
   1.3 Security in WMNs ................................................................. 12
   1.4 Thesis Organization .......................................................... 13

2. Related Work .......................... 14
   2.1 Related Work ................................................................. 14

3. Network model and problem formulation .......................... 18
   3.1 Network Architecture ................................................................. 18
   3.2 Key establishment and mobile authentication .................................... 20
   3.3 Key Distribution Methods ............................................................. 21
      3.3.1 Symmetric Polynomial based key Distribution .................................. 21
      3.3.2 Asymmetric Function based key Distribution .................................... 22

4. Distributed Authentication, Key Generation and Establishment .......................... 24
   4.1 Individual Domain Function Generation ............................................. 25
      4.1.1 Inter MR-MC Hierarchical Hybrid-symmetric Domain Function generation ............................................. 25
      4.1.2 Inter MC-MC Hierarchical Symmetric Domain Function Generation ............................................. 25
   4.2 Cooperative Federated function initialization and distribution ................. 26
   4.3 Individual function initialization and distribution .................................. 27
      4.3.1 Inter MR-MC Function Initialization ............................................. 27
      4.3.2 Inter MC-MC Function Initialization ............................................. 28
   4.4 Authenticated pairwise master key generation ...................................... 29
      4.4.1 Authenticated Key Generation between MR and MC .......................... 29
      4.4.2 Authenticated key Generation between MCs .................................... 31
## CONTENTS

4.5 Pairwise Session Key Generation .................................................. 32

5 Security and performance of HMSF-AKE ....................................... 34
  5.1 Security properties of HMSF-AKE ............................................ 34
  5.2 Security analysis ................................................................. 35
  5.3 Efficiency enhancement at AAAs ............................................ 35
  5.4 Computational overhead and Latency performance Evaluation ........ 37

6 Conclusions and Future Work ..................................................... 44
  6.1 Conclusion ........................................................................... 44
  6.2 Future Work ........................................................................ 44
List of Figures

1.1 Wireless Mesh Network ................................................................. 10
3.1 WMN architecture ..................................................................... 19
4.1 AAAs ID exchange for MR-MC .................................................... 26
4.2 AAAs ID exchange for MC-MC ..................................................... 27
4.3 Function distribution to MRs and MCs ......................................... 28
4.4 Function distribution to MCs ......................................................... 29
4.5 MR-MC Key generation ................................................................. 30
4.6 MC-MC Key generation ................................................................. 31
4.7 Pairwise Session key generation ................................................... 33
5.1 Coefficient selection probability ................................................... 36
5.2 Authentication Latency with varying MR-IGW hops ......................... 40
5.3 Authentication Latency with varying traffic ......................................... 41
5.4 Proposed HMSF-AKES scheme against HLR-VLR Scheme for varying no. of hops 42
5.5 Proposed HMSF-AKES scheme against HLR-VLR Scheme for varying traffic 43
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Latency with number of hops</td>
<td>39</td>
</tr>
<tr>
<td>5.2</td>
<td>Latency with different traffic rates</td>
<td>40</td>
</tr>
<tr>
<td>5.3</td>
<td>4 way handshake between the Mesh Client and Mesh Router for HMSF-AKES Scheme</td>
<td>41</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Wireless Mesh Networks

Wireless Mesh Networks (WMN) is a promising wireless technology that complements high bandwidth communication connectivity of a wired infrastructure with wireless backbone for the mobile nodes (MNs). Different from flat network architectures such as an ad-hoc network, WMN is primarily hierarchal network architecture. The network essentially comprises of mobile nodes or clients in the lowest level, wireless mesh routers in the intermediate level and gateways connected to internet servers at the highest level. In an attempt to standardize the WMN technology, the IEEE 802.11s has been consistently working on the mesh network ingredients till date. The mesh network depends on the multi hop communication technique for the traffic to and from underlying devices.

Unlike traditional Wi-Fi networks, the Access point (AP) need not be wired completely for its functionality. The APs that are connected to the wired network in WMNs are referred to as Mesh Portals (MPP) or the internet gateways (IGW). The other wirelessly connected APs are coined as Mesh Access Points (MAP) or simply Mesh Router (MR). The clients or the nodes that attach to these MAP are simply known as the client stations (STA) or Mesh Clients or Mobile Clients (MC). The term however could be used interchangeably. The MPP are essentially MAPs which have wired high speed connection link to the internet to allow the traffic in and out of the WMN. The remaining MRs interconnects to each other wirelessly and communicates in a multi-hop fashion using different multi-hop protocols in different layers. Finally, The MCs at the lower level of hierarchy are serviced by the MRs. To summarize, the WMN is a wireless network with MRs forming a wireless backbone to provide high band width Internet connectivity to its clients. Figure 1.1 illustrates a basic structure of WMN.
Figure 1.1: Wireless Mesh Network
1.2 Application of wireless mesh networks

Low cost deployment and high speed internet connectivity add attractive features to WMNs which can be used for a number of applications. Moreover, the wireless MRs are relatively static and have an advantage of no power constraints [1]. Few commercial applications of the WMN are listed below.

Internet due to different traffic model that primarily exists between MRs and IGWs [1] for high speed communication, WMNs are able to support them effectively over the network. The IGWs are hard wired to the internet and hence offering high bandwidth than traditional wireless LAN.

High speed connectivity in the network for multimedia applications gives more flexibility to the multimedia features in the network. Applications such as VOIP, streaming video, etc which have high QoS requirement can be implemented in a WMN with much smaller hassle than the traditional wireless network.

WMNs provide an easy and cost effective solution to equip the city for an intelligent transport system [2] so as to implement effective information delivery systems through roadways. The vehicles equipped with system will be able to provide real time travel information to the passengers not only at their current location, but also for other locations around the city. In such an attempt, Mesh Networks Inc has established Portsmouth Real-Time Travel Information System (PORTAL), equipping more than 300 buses with the WMN technology. At any given time the passengers can have the travel information for more than 40 locations from their current location.

In terms of ease of deployment and cost effectiveness, WMNs have proven to be superior to traditional cellular infrastructures in terms of public safety. WMNs provide much higher data rates as compared to the cellular infrastructure, allowing more information to be passed in and out of the network, that to with high speed. For any agency, such as law enforcement offices and government offices it is not cost effective to have an independent cellular infrastructure. Thus, in such corporations WMNs have become a natural solution. Such an example can be found in San Mateo Police Department in San Francisco Bay Area where the vehicles are equipped with laptops and patrol bicycles with PDAs for communication using WMN.[2]

Public Internet Access WMNs can be used to provide broadband wireless connectivity publicly, indoors or outdoors in urban and rural areas by eliminating the use of costly wired network infrastructure. An example of this can be found in Cerritos, California where Aiirmesh Communications Inc activated a metro scale wireless broadband connectivity turning the city Wi-Fi.[2]
1.3 Security in WMNs

The dynamically changing topology, lack of conventional secured infrastructure and open medium of communication make WMNs extremely susceptible to intruders as compared to a wired network [3]. The topology of the network is constantly changing, as the MCs are roaming from one domain to another domain and the nodes are constantly leaving and entering the domains of the WMN. We need a fast and efficient way of secured handoff. The MCs entering the network should not be able to derive the key beforehand and the one that are leaving should not be able to use the key in the network next time they visit again. A number of security or authentication features are available to date. Broadly, the security feature can be classified as

1. Asymmetric cryptography or Public key cryptography, and

2. Symmetric key cryptography.

Public key cryptography or an Asymmetric cryptography provides a robust scheme of secured communication. With the most powerful number theoretic technique, it is infeasible to crack them, even by making use of the supercomputers. Public key cryptography basically makes use of two keys: A Public key ($K_u$) and A Private key ($K_r$). $K_u$ is available publically whereas $K_r$ is known only to a specific entity. By communicating the nodes make use of the $K_u$ and $K_r$ for authentication, confidentiality and digital signature purpose. The scheme is very attractive for all such characteristics. However, in WMNs, MCs are not necessarily a powerful computer to handle complex numbers. Even if MCs are capable of it, they exceed the timing benchmark set for the QoS of WiMAX kind of applications. For example, Extensible Authentication Protocol (EAP) provides robust authentication infrastructure between the clients and authentication servers. However, the protocol is quite complex and establishing the authentication of a roaming MC is not feasible when it moves from its registered domain to a visiting domain or quickly extending an ongoing session to a new session. This also implies a lot of overhead. For aforementioned reasons, WMNs look for symmetric key cryptography as a viable solution. Symmetric key cryptography makes use of a single key ($K$) for a secure communication among the two entities. One of the popular symmetric key schemes is the Dee Hellman scheme where both the parties share a small piece of information. Then, the communication entities make use of this shared piece to derive the keys independently which is then used for a secure communication. Here, we focus on the authentication aspect of the security feature in WMNs by following the principles of symmetric key cryptography. The WMN consists of various other sub networks which may be handled by different Internet service providers (ISPs). When a MC roams around this network
from its home domain, it is necessary to have a fast and efficient form of authentication to build a trust relationship in the visiting domain. The MC needs to do mutual authentication and confidentiality between it and the MRs. We also discuss a simple and naïve approach of establishing temporary session keys between a pair of MCs whenever they want to communicate among each other. Furthermore, a distributed version of AAA servers makes the entire scheme more robust and less susceptible to the intruder.

1.4 Thesis Organization

This thesis is organized into a total of 6 chapters. Chapter 1 gives a brief introduction of the WMNs and the need for security. Various applications where WMNs are used are mentioned in this chapter. The differences between symmetric cryptography and public key cryptography have also been mentioned, and the need for the type of cryptography for fast and efficient mutual authentication in WMNs that could meet QoS requirements is also indicated.

Chapter 2 gives an overview of the related work. Chapter 3 provides an insight to the scheme is being deployed the WMN. The hierarchal structure of the network and other terminologies are defined. We also give an overview of an authentication scheme between MR-MC and MC-MC within the same domain or between multiple domains. Chapter 3 also provides various types of Key distribution methods. Chapter 4 introduces our Authentication scheme for a WMN. Chapter 4 is the heart of the thesis as it provides with detailed analysis of distributed authentication, key generation and key establishment between two end entities. Here, we discuss the symmetric polynomial function and implement the same in the network as introduced in Chapter 3.

Chapter 5 evaluates the efficiency and performance of our proposed scheme and its associated properties. The chapter also contains of simulation results. Finally, in Chapter 6, we provide our future work and conclusions.
Chapter 2

Related Work

2.1 Related Work

K. Khan and M. Akbar in [4] proposed a scheme for multihop WMNs. Their scheme is primarily based on the extension of scheme proposed by Paul Funk in [5]. They name their proposed scheme as EAP-TTLS (Tunneled Transport Layer Security). The layered protocol model basically consists of two phases. First, a TLS handshake phase, where the actual authentication process takes place between a server and client or vice-versa, and second the TLS tunnel phase, which establishes a secure tunnel between the communicating nodes for exchange of other related information. The scheme is robust in nature in a sense that it makes use of multiple challenge response steps. Furthermore it has a choice as to which authentication protocol such as MD5, Password Authentication Protocol (PAP), etc may be used for the authentication process.

Another EAP based authentication mechanism for multihop WMNs is described in [6] by F. Fitzek et al. They make use of the UMTS Authentication and Key Agreement (UMTS-AKA) in accordance with EAP and call the scheme as UMTS-AKA over EPA. In this scheme, the already authenticated client known as authenticator authenticates the incoming new node to the network. During the initial phase, the authenticator first receives the client ID of the incoming node. The authenticator then connects to the AAA server and gathers the required information for the authentication process. The authenticator retrieves the information from the Home location register (HLR) of the incoming client. Initially the Visitor location register (VLR) where the authenticator needs to sends request to the HLR of the visiting client. As a response, HLR sends a set of authentication vectors to the VLR. On receiving this information, VLR sends authentication request to the terminal along with a random challenge and an authentication token and passes it to the authenticator. In turn, authenticator authenticates the new client in the network.
Even this EPA schemes look attractive and robust, it is not bandwidth efficient and does not minimize the overhead in a multi hop WMNs. However, such an authentication is infeasible in our scheme as we have tight constraints on latency/jitter and has limited QoS flexibility. Furthermore, most of these schemes either do not support the mobility of a station or the requirement of extending the ongoing session with the current AP to another domain, quickly before it expires.

Hur et al. in [7] propose a pre-authorization scheme to support accelerated entry from one domain to another. The authors modify the existing key management of Privacy Key Management (PKMv2) slightly, which enables the MC to establish an authorization key (AK) before hand o to the neighboring Base stations (BS) in the diversity set. The established key maintains both the forward secrecy and the backward secrecy. Two separate methods have been designed on the premise of the hand o technique. First, the pre-authentication scheme for Hard Handover and second, the pre-authentication scheme for a Soft Handover. Both the schemes have a policy of sharing the keys among the neighboring BSs in the initial phase during communication before hand off. In order to solve resulting domino effect due to sharing of keys among BSs, authors make use of the least privilege principle, which implies each entity to know the least amount of information for continuation of the operation. The scheme provides a robust technique for an accelerated entry between the domains and supports single hop architecture. Our scheme involves multi hop communication and thus the design parameters cannot do such support.

Most of the schemes designed for a conventional single hop network cannot be applied to WMNs either because of the architecture or because of the scheme, as it cannot resist to malicious attacks [8]. In [8] Zhou et al. analyze the security flaws of the existing IEEE 802.16 in mesh networks, identify the security flaws and propose some solutions to deal with the attack. Whenever a candidate node wants to get access to the network, it sends a series of request messages to the Authorization center. The initial handshaking signal contains the X.509 certificate of the candidate node issued by the manufacturer. On receiving the message from the candidate node the Authorization center verifies the certificate with the public key of the manufacturer. In case of a failure, the candidate node, i.e. the MC is notified with a string of error code. In case of a success, the authorization center responds with authorization key, its lifetime, Operator Shared Secret (OSS) and other related information. All of these transactions take place via a sponsoring node that tunnels the information between the candidate and the authorization center. The OSS is used as a global key shared by all the nodes in the network. It can be used by candidates to establish a link or gain access to the network. Because of this universal property, the OSS is vulnerable to an attacker, which could completely disrupt the network. Authors provide a naïve solution to the problem. The design of mesh certificates during the authorization process and a series of challenge-response handshake signals and nonce would make the system less susceptible to the attackers. Whatever the case may be, any of the above mentioned cases make use of public key cryptography and causes a large computational overhead in a mobility scenario.
In [9], Lee et al. discuss the authentication mechanisms in Wireless distributed System (WDS), with the basic principle of having a number of trusted nodes (TN) being deployed in the network. The trusted nodes are basically nothing but the APs. This way every time the MC need not have to communicate with the central AAA server for determining the key in the network. Whenever a MC wants to communicate with an AP with no prior security association and no shared secret, the AP broadcasts the identity of MC to the WDS, in order to find any other AP within the WDS which could recognize the MC. In case of a failure, the MC would not be able to get itself authenticated. In the other case, it tries to determine how many hops away the AP is from the TN. In both of these cases, reactive routing protocol is used to find the TN and the key distribution protocol acts accordingly. The authentication of new MC is possible even when it does not have a pre-shared key with its immediate neighbor or AP does not communicate to the central AAA server. Due to the availability of distributed authenticating entities in the network, the proposed scheme has lower authentication overhead as compared to a centralized architecture. As the number of TN increases in the network, the authentication delay decreases due to distribution of authentication traffic which in turn positively affects the entire network performance. In the other hand, as the number of MCs increases the load in the network increases, affecting the overall time required for authenticating process.

Soltwisch et al. in [10] a new way of establishing security association between any two Access routers (ARs). The mechanism presented is an improved version of Context Transfer Protocol (CTP), which possesses seamless handover property for the MCs. When a MC links from the previous AR (pAR) to new AR (nAR), as it is faster and efficient to contact pAR than the home network. The CTP supports the hand over scheme in scenarios of the same domain i.e., when both the ARs are in the same network and does not hold well for the inter domain handover. Thus, the authors propose an Inter Domain-Key-Exchange (IDKE) that addresses the issue of seamless IP inter domain hand off. The main objective of IDKE is to provide security related features such as encryption and authentication by establishing a trust relationship and a shared secret key between MC and nAR. Instead of re-establishing the keys right from the scratch, it simply forwards the key from pAR to nAR. Prior to this phase, security association is established between nAR and pAR. The proposed mechanism has advantages over various other technologies such as the GSM and EAP based authentication scheme. The scheme is faster and the overall bandwidth consumption is relatively small.

As discussed earlier, most of the schemes provide a robust and efficient authentication. The main drawback of these schemes are either they are too complex to be implemented in a WMN with strict time constrains or they do not support the hierarchal architecture design of a WMN. Either they lack the multi hop approach or an important hand over of MCs between different service domains. Neither has the issue been considered when two MCs need to communicate with each other.
In [11] Gupta et al. provides a key generation and authentication system in cellular-based Mobile Ad Hoc Network (MANET). The decentralized mechanism for key generation makes use of a symmetric polynomial that is initiated by the BSs itself. The scheme is supplemented with both the forward and backward secrecy, along with decentralized scheme which makes it less vulnerable to different attacks. Once the keys are passed on to the MCs, they are capable of establishing pair wise key without any intervention from the BS, thereby reducing the overall management cost at the BS. This thesis is motivated by the concept introduced in [11]. It provides a generalized version a symmetrical multi variate polynomial and touches other issues not covered earlier. The idea has been extended to WMN where each entity of the network is capable of establishing authentication keys by the usage of a function.
Chapter 3

Network model and problem formulation

3.1 Network Architecture

A WMN primarily comprises of mesh routers (MRs) as the backbone of the network. The main function of the MRs is to collect data at MC, the lower level of hierarchy. An IGW connects the network to the outside world through access to the Internet. In MANETs, the traffic is generally between the mobile nodes. However, in the case of WMNs the traffic is predominantly directed to or from the IGW. Figure 3.1 shows a generalized version of the network architecture for WMN used in our study. As seen in the Figure 3.1, a hierarchal structure is present as the network architecture. The communication traffic is routed amongst the MRs and finally transferred to the IGWs as the level of the hierarchy IGWs finally for the delivery. Similarly, all the downlink traffic in the network commence at the IGW which provides Internet Access to the MRs and around its premise. More the number of IGWs, less will be the constraints on load balancing. For a large coverage area, different Internet Service Providers (ISPs) may maintain different WMN. WMN belonging to a particular ISP is known as administrative mesh domain of an ISP or simply an ISP domain. Each of the ISP domains may have one or more IGWs in them providing connection to the MRs. For a MC to have access to a website, it is necessary for them to connect to the WMN and be registered to one of the ISP domain. This is similar to the GSM networks where the client needs to register itself in the Home Location Register (HLR). Once the MC registers in that particular ISP domain, it becomes their home domain. Moreover, each of the ISP domains maintains a central administrative center, which controls the authentication, authorization and administrative (AAA) functions in the network. We call the central administrative center here as an AAA server which functions similar to that of the RADIUS protocol used in wireless LANs. The AAA server at the backend of WMN is unique to the ISP and contains all the required information related to its clients, namely the identifier, registration information of the client, billing, location,
Figure 3.1: WMN architecture
permissions and security level.

Situations may arise when the mesh client served by one ISP domain needs to enter another ISP domain. In such a case, it is necessary to have a mutual coordination between two or more mesh domains. When two or more mesh domains couple each other for the mutual benefits we call it as a federation. In this way, MCs can belong to a federated domain, which provide seamless Internet access.

As seen in the Figure 3.1 we have two ISP domains, $D_i$ ($i=1$ to $2$). The AAA server in domain $D_i$ has the unique ID = $i$ of the domain. Thus AAA ($i=1$ to $2$) belongs to the respective $D_i$. $D_1$ belongs to ISP$_1$ and $D_2$ to ISP$_2$. $D_1$ consists of AAA$_1$ and $D_2$ has AAA$_2$. AAA$_i$ is in charge of IGW$_1$ and IGW$_2$. On the other hand, AAA$_2$ provides authorization, accounting and authentication to IGW$_2$. The MRs are associated with the IGWs belong to that specific domain, and the MCs to that MRs which is their actual home domain in the network.

The major abbreviations used are:

- $ISP_i$: Internet service provider in a WMN with ID $i$
- $D_i$: Mesh domain of $ISP_i$
- $D$: Set of domains in a WMN with N domains, $D = \{D_1,D_2,...........D_N\}$
- AAA$_i$: AAA server in domain $D_i$ of $ISP_i$
- MR$_j$, MR$_{ij}$: Mesh router with ID $j$, and $i$ denotes the ISP. $ISP_i$ it belongs to.
- MC$_j$, MC$_{ji}$: Mesh client with ID $j$, and $i$ denotes its home domain $ISP_i$
- $K_m(A, B)$: Pairwise master key between two entities A and B.
- $K_s(A, B)$: Pairwise session key, which is derived from $K_m(A, B)$.

3.2 Key establishment and mobile authentication

Authentication key establishment (AKE) is one of the most important aspects of the network security. As discussed earlier, a number of different techniques exist for key generation in a single hop networks. Whilst in the case of a multi hop WMN, key establishment is more vital in terms of security because of the hierarchal architecture they follow. Furthermore, in a federated WMN, various sub-networks belong to various ISP domain, and there exist no single central authority (such as AAA) to regulate the entire
federation or individual ISP domains. Having a single centralized authority for key generation turns out to be more risky. The MCs may be moving between different ISP domains and MCs would not be able to securely communicate in a domain different from where it is registered.

The key establishment procedure in our scenario consists of two distinct problems. First, the authentication between a MC and a MR, and second the authentication required when ever two MCs need to communicate with each other.

In the first case we may have situation a new MC trying to join a mesh domain in WMN. The MR needs to validate MC it wants to serve. We should be sure that the requesting MC is not an adversary. Furthermore, MC can move from one MR to another within the same or different ISP domain. The second is the inter-MCs communication where MCs willing to communicate may belong to the same or different domains. Here, we focus on these basic definitions and consider how any two entities could have a shared key for security. Therefore, it is necessary for the establishing authentication key to provide secure communication in the federated WMN between any two participating entities which could be between MCs or between MR and MC. In general, the scheme should be able to fulfill the following security features in the network as discussed in [12].

The accessed MR can authenticate the MC. The roaming MC can authenticate the MR. Two MCs can authenticate each other. MR and MC can setup a shared secret key for communication. Two MCs can setup a shared secret key to communicate. Apart from the above authentication related issues, the scheme should also take into consideration the QoS involved especially WMN with high bandwidth. The authentication should not be an overhead in the network. Also, the MCs and MRs must be capable of establishing the key efficiently and with smaller delay.

3.3 Key Distribution Methods

3.3.1 Symmetric Polynomial based key Distribution

Symmetric key generation scheme (SKGS) was first proposed by Blom in [13], where a pair of sensor nodes (SNs) establishes a common key between them. The same secret key is used by the nodes for the secure communication between them. The amount of secret information they exchange between them is the least. An authorized server such as AAA distributes a piece of information to the network entity and the users are capable of computing a shared secret using it. The piece of information passed is nothing but symmetrical polynomial. Once the users receive this information, they may substitute their respective unique IDs to produce a common secret key. In [14], Blundo et al. proposed a secure key distribution scheme for a dynamic
conference, which is an extension of [13]. In this scheme the nodes or MCs may leave or enter the network making it dynamic in nature. As the topology is not fixed, a t-degree bivariate symmetric polynomial based pre-distribution scheme is proposed which is equally applicable in a hierarchical network. The scheme is called k-secure, where k is the degree of symmetric polynomial. The authors provide a rigorous analysis and show the robustness of the scheme. In symmetric polynomial based key distribution scheme the Authentication server generates a k-degree bivariate polynomial given by:

\[ F(x, y) = \sum_{i,j=0}^{k} a_{i,j} x^i y^j \] ...................................................... (3.1)

where,

Coefficients \( a_{i,j} \) (\( 0 \leq i, j \leq k \)) are chosen randomly from a finite field \( \mathbb{F}_q \) and \( q \) is a large prime number.

By choosing appropriate coefficients \( a_{i,j} = a_{j,i} \) the bivariate polynomial is symmetric in nature such that,

\[ F(x, y) = F(y, x) \] ...................................................................(3.2)

We assume that all the entities of the network have unique IDs. Whenever the authentication server wants to pass the information to a node, it evaluates the function \( f(x, y) \) with its ID \( i \) as \( x = i \). The entity with ID= \( j \) receives the function \( f(i, y) \). Similarly, let us consider another node with ID= \( j \) that receives the polynomial function \( f(j, y) \) by the evaluating \( f(x, y) \) with \( x = j \). In both the cases, no one has the information about the originally generated polynomial in the authentication server. Both the nodes with ID= \( i \) and ID= \( j \) do not have complete information about the original polynomial. Now, whenever the two nodes want to communicate with each other, they generate a common shared key for communication using symmetric nature of the polynomial. For example, when node having the function \( f(i, y) \) wants to initiate a communication it evaluates \( f(i, j) \) and node having the function \( f(j, y) \) individually evaluates \( f(j, i) \). The symmetric nature of polynomial makes:

\[ f(i, j) = f(j, i) \] .......................................................................(3.3)

and the derived value can be used as a shared symmetric key between any two nodes. The pair wise shared secret could thus be obtained for the secure communication.

3.3.2 Asymmetric Function based key Distribution

Polynomial based key generation scheme can be extended to asymmetric function for mutual authentication and key establishment between any two entities belonging to different hierarchies. In other words, we can state that the asymmetric function can be used to provide validation between any two entities that are not same or identical. For example, case of WMNs, we may use a function for authentication between the MRs and MCs. This is not as the same while using symmetric functions which that is useful for doing authentication between equal entities in the same hierarchy, such as only between the MCs. The usage of
asymmetric function will not only allow MR to authenticate the identity of MC, but also validate the status. This means MRs cannot claim themselves as MCs. The status validation in our scheme allows identifying the server to verify the type of user in the federated domain. Similar to the symmetric polynomial scheme, the authentication server first generates a bivariate function \( f(x, y) \) in a secure manner, after reserving the use of variable \( x \) for the MRs and the second variable \( y \) for the use of MCs. The function is then passed on to the MR and MC by substituting their respective IDs. Let us consider a scenario with MR\(_i\) having an ID as \( i \) and MC\(_j\) with a unique ID \( j \). The authentication server takes the following steps in distributing the function:

1. Generates the function \( g_i(y) = f(i, y) \), by evaluating \( f(x, y) \big|_{x=i} = g_i(y) = f(i, y) \) for MR\(_i\) with ID \( i \)
2. Generates the function \( h_j(x) = f(x, j) \), by evaluating \( f(x, y) \big|_{y=j} = h_j(x) = f(x, j) \) for MC\(_j\) for the MC with ID \( j \)

Both MR\(_i\) and MC\(_j\) have no knowledge of the original polynomial function. Whenever the two unequal entities want to communicate, they evaluate the passed function to them with the corresponding ID of the other entity to obtain a symmetric key. In the above described case, MR\(_i\) evaluates \( g_i(y) \) using the identity of MC\(_j\), i.e., with \( y = j \)

\[
\text{Key}(\text{MR}_i, \text{MC}_j) = g_i(y) \big|_{y=j} = f(i, j) \tag{3.4}
\]

Similarly, the MC\(_j\) evaluates the function \( h_j(x) \) using the identity of MR\(_i\) at \( x=i \) as

\[
\text{Key}(\text{MC}_j, \text{MR}_i) = h_j(x) \big|_{x=i} = f(i, j) \tag{3.5}
\]

From Eq.(3.4) and Eq.(3.5), we have

\[
\text{Key}(\text{MR}_i, \text{MC}_j) = \text{Key}(\text{MC}_j, \text{MR}_i) \tag{3.6}
\]

The key generated above would serve as a key for communication between any two unequal entities. The key is obtained by independent calculations in the individual entities itself and neither of them has an idea about the original function generated by the authentication server. Using the same key, mutual authentication and status validation could also be performed.
Chapter 4

Distributed Authentication, Key Generation and Establishment

Based on a symmetric polynomial function and the asymmetric polynomial function discussed in the previous chapter, here we propose a naive approach for using them in a WMN. We call our scheme as Hierarchical Multivariable Symmetric Functions based Authenticated Key Establishment (HMSF-AKE) scheme. Using the properties of the functions here we design two distributed authentication and key establishment schemes, namely between MR and MC (MR-MC AKE) and between two MCs (MC-MC AKE). Various phases of distribution, process for the final key generation is established in different domain scenarios and can be given as follows:

- Individual domain function generation.
- Cooperative Federated function initialization and distribution
- Individual function initialization and distribution
- Authenticated pair wise master key generation.
- Pair-wise session key generation

We discuss each of the procedures briefly in this chapter.
4.1 Individual Domain Function Generation.

We know that, a WMN may comprise of one or more ISP domains or multiple mesh domains. From the network model described in the previous chapter each ISP has its own AAA server to provide the service to the specified ISP domain. Furthermore, the entities of WMN, i.e., the MRs and MCs have a unique non-zero IDs associated with them.

4.1.1 Inter MR-MC Hierarchical Hybrid-symmetric Domain Function generation

During this phase, each of the AAA in their respective domain generates a \( t \)-degree four variate two level hierarchical domain function \( f_i(v, w, x, y) \). The function \( f_i \) represents the function generated by AAA, belonging to the ISP domain \( i \). The function can further be defined by a polynomial representation as:

\[
f_i(v, w, x, y) = \sum_{i,j,m,n=0}^t a_{i,j,m,n} v^i w^j x^m y^n. ................................................. (4.1)
\]

The coefficients \( a_{i,j,m,n} \) are chosen over a finite field \( F_q \) where \( q \) is a large prime number. The coefficients \( a_{i,j,m,n} \) are randomly selected by the AAA server and are independent and without correlation between them. Higher the degree \( t \) of the polynomial is, more robust it is going to be. With the appropriate choice of the coefficients \( a_{i,j,m,n} = a_{i,j,n,m} \), the polynomial functions can have the desired symmetric property. Thus:

\[
f_i(v, w, x, y) = f_i(v, w, y, x). ......................................................... (4.2)
\]

In eq. (4.1) the variable \( v \) will be used for the MC, and variable \( w \) is reserved ID for the MR. The other two variables \( x \) and \( y \) are used by the AAA servers of the same or different domain during the initial polynomial distribution process. This constraint on the usage of variables for specific node ID (\( v \) for MC, \( w \) for MR and \( x, y \) for AAA) reflects the hierarchal network architecture of WMN.

4.1.2 Inter MC-MC Hierarchical Symmetric Domain Function Generation

Similar to the phase described above the AAA server generates another \( t \)-degree four variate two-level hierarchical domain function \( g_i(p, q, x, y) \). The function can be further defined by polynomial representation as,

\[
g_i(p, q, x, y) = \sum_{i,j,m,n=0}^t b_{i,j,m,n} p^i q^j x^m y^n. ......................................................... (4.3)
\]

With the appropriate choice of the coefficients, \( b_{i,j,m,n} = b_{i,j,n,m} \) and \( b_{i,j,m,n} = b_{j,i,n,m} \).............. (4.4) the polynomial functions will have the desired symmetric property. Thus, we can state that

\[
g_i(p, q, x, y) = g_i(q, p, x, y). ......................................................... (4.5)
\]

and,
4.2 Cooperative Federated function initialization and distribution

After generating two domain functions, the AAA server initiates the distribution process. Each AAA server securely transmits the two functions $f$ and $g$ to all other AAA server in the WMN. We assume that the communication between AAAs takes place in a secured, high speed, pre authenticated channels. Here, the total number of function transmitted by a single AAA equals to $n - 1$ functions, in WMN with $n$ AAAs. For further understanding let us consider the scenario below for MR-MC domain function.

As shown in Figure 4.1, we have two AAA servers, $AAA_i$ and $AAA_j$, representing the AAAs in two separate domains $i$ and $j$. $AAA_i$ generates function $f_i(v, w, x, y)$ and transmits it securely to $AAA_j$ by evaluating,

$$f_i(v, w, x, y)|_{y=j} = f_i(v, w, x, j). \quad (4.7)$$

Similarly, $AAA_j$ generates function $f_j(v, w, x, y)$ and transmits it securely to $AAA_i$ by evaluating:

$$f_j(v, w, x, y)|_{y=i} = f_j(v, w, x, i). \quad (4.8)$$

After the distribution process, each $AAA_i$ will have the functions from all other cooperative AAAs and obtains the federated MC-MR function as:

$$F_i(v, w, x) = \sum_{k=1}^{N} f_k (v, w, x, i). \quad (4.9)$$

In a similar manner, the federated MC-MC domain function for the AAA is obtained as follows:

As shown in Figure 4.2, we have two AAA servers, $AAA_i$ and $AAA_j$, representing the AAAs in two separate domains $i$ and $j$. $AAA_i$ generates function $f_i(v, w, z, y)$ and transmits it securely to $AAA_j$ by evaluating,

$$f_i(v, w, z, y)|_{y=j} = f_i(v, w, z, j). \quad (4.10)$$

Similarly, $AAA_j$ generates function $f_j(v, w, z, y)$ and transmits it securely to $AAA_i$ by evaluating:

$$f_j(v, w, z, y)|_{y=i} = f_j(v, w, z, i). \quad (4.11)$$

After the distribution process, each $AAA_i$ will have the functions from all other cooperative AAAs and obtains the federated MC-MC function as:

$$F_i(v, w, y) = \sum_{k=1}^{N} f_k (v, w, z, i). \quad (4.12)$$

In a similar manner, the federated MC-MC domain function for the AAA is obtained as follows:
CHAPTER 4. DISTRIBUTED AUTHENTICATION, KEY GENERATION AND ESTABLISHMENT

Figure 4.2: AAAs ID exchange for MC-MC

separate domains $i$ and $j$. $AAA_i$ generates function $g_i(p, q, x, y)$ and transmits it securely to $AAA_j$ by evaluating:

$$g_i(p, q, x, y)_{y=j} = g_i(p, q, x, j). \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdOTS

4.3 Individual function initialization and distribution

Each of the MRs and MCs are registered with AAA in their home domains. The MR and the MC receives service from their respective AAA server where they have their initial information available. This subscription process provides a roaming mode to the MCs in different mesh domains of the WMNs. In this section, we discuss the function initialization process between MR-MC or between two MCs.

4.3.1 Inter MR-MC Function Initialization

The AAA server receives the federated function $F(i)$ after collecting the individual functions from all other AAA. It evaluates it by making use of the ID of its subscribed customer. Let us consider a sample scenario shown below Figure 4.3.

Here, we have two AAA servers in two different mesh domains namely $AAA_i$ and $AAA_j$. The federated function available to $AAA_i$ and $AAA_j$ from the previous stage are $F_i(v, w, x)$ and $F_j(v, w, x)$ respectively.
The AAA servers evaluate the functions for their MRs and MCs. Here, $MR_i$ and $MR_a$ have $AAA_i$ as their home domain and are represented as $MR_{i,l}$ and $MC_{a,l}$ where $l$ and $a$ are the unique IDs of MR and MC respectively and $i$ represents the domain they belong to.

The $AAA_i$ now evaluates $F_i(v, w, x)\mid_{v=a}$ by substituting $v$ for the ID $a$ of $MC_{a,l}$. Hence, the function received by $MC_{a,l}$ is,

$$F_{MC(a,l)}(w, x) = F_i(v, w, x)\mid_{v=a} = F_i(a, w, x)$$

.....................................................(4.13)

$AAA_i$ evaluates the federated function $F_i(v, w, x)\mid_{w=l}$ by substituting $w$ for the ID $l$, of MR. Hence, the function received by $MR_{l,i}$ is,

$$F_{MR(l,i)}(v, x) = F_i(v, w, x)\mid_{w=l} = F_i(v, l, x)$$

.....................................................(4.14)

In a similar fashion the functions evaluated by $AAA_i$ for $MC_{b,j}$ and $MR_{k,j}$ are as follows:

$$F_{MC(b,j)}(w, x) = F_j(v, w, x)\mid_{v=b} = F_j(b, w, x)$$

.....................................................(4.15)

$$F_{MR(k,j)}(v, x) = F_j(v, w, x)\mid_{w=k} = F_j(v, k, x)$$

.....................................................(4.16)

### 4.3.2 Inter MC-MC Function Initialization

As described in the previous section, the AAA server also receives federated MC-MC function $G()$. In a similar fashion the MC of a particular domain obtains Inter-MCs function from the AAA.

In the Figure 4.4, the federated MC-MC function available to $AAA_i$ and $AAA_j$ from the previous stage are $G_i(p, q, x)$ and $G_j(p, q, x)$ respectively. The AAA servers evaluate the functions for their MCs. Here, $MC_a$ has $AAA_i$ as its home domain and is represented as $MC_{a,i}$ where $a$ is the unique ID of MC and $i$ represents the...
domain it belongs to. By substituting $p$ for the ID $a$, the AAA$_i$ now evaluates $G_i(p, q, x)|_{p=a}$. Thus, the function received by $MC_{a,i}$ is:

$$G_{MC(a,i)}(q, x) = G_i(p, q, x)|_{p=a} = G_i(a, q, x)$$

(4.17)

At the same time, AAA$_j$ evaluates the federated function $G_j(p, q, x)|_{p=b}$ by substituting $p$ for the ID $b$, of MC. Hence, the function received by $MR_{i,j}$ is,

$$G_{MC(b,j)}(q, x) = G_j(p, q, x)|_{p=b} = G_j(b, q, x)$$

(4.18)

### 4.4 Authenticated pairwise master key generation

#### 4.4.1 Authenticated Key Generation between MR and MC

When MC and MR want to communicate to each other, they make use of the federated function available to them from the previous stage. Both the MR and the MC substitute their respective IDs in the variable reserved for them by the AAA server. Let us consider a scenario when $MC_{a,i}$ enters the radio range of $MR_{b,j}$ and wants to communicate with it. Here, $MC_{a,i}$ has ID $a$ and is registered to home AAA$_i$, while $MR_{b,j}$ has a unique ID $b$ and registered to the home domain AAA$_j$. The same key generation process works when both the MR and MC belong to the same domain.

Initially the $MC_{a,i}$ carries the following function:

$$F_{MC(a,i)}(w, x) = F_i(a, w, x)$$

(4.19)

Similarly, $MR_{b,j}$ follows the function:

$$F_{MR(b,j)}(v, x) = F_j(v, b, x)$$

(4.20)

Now, whenever the MC wants to establish a connection with the MR, MC uses the ID $b$ of the MR
for \( w \) and the home domain address of MR i.e. \( j \) in place of \( x \). The polynomial is thus reduced to a single number which can be used for the purpose of secure communication. The obtained information by \( MC_{a.i} \) is the evaluation of the polynomial function is used as a pair wise master key with \( MR_{b.j} \) as:

\[
K_m(MC_{a.i}, MR_{b.j}) = F_{MC(a.i)}(w, x)|_{w=b, x=j} = F_i(a, w, x)|_{w=b, x=j} = F_i(a, b, j)
\]

In a similar manner, the MR evaluates the key by substituting the ID= \( a \) and the domain address of MC i.e., \( i \) in its federated domain function \( F_j(v, b, x) \) in place of \( v \) and \( x \) respectively. The pair wise master key obtained by \( MR_{b.j} \) with \( MC_{a.i} \) is evaluated as follows,

\[
K_m(MR_{b.j}, MC_{a.i}) = F_{MR(b.j)}(v, x)|_{v=a, x=i} = F_j(v, b, x)|_{v=a, x=i} = F_j(a, b, i)
\]

**Proof of symmetry:**

From Eq. 4.9, we have

\[
F_i(a, b, j) = \sum_{k=1}^{N} f_k(a, b, j, i)
\]

and,

\[
F_j(a, b, i) = \sum_{k=1}^{N} f_k(a, b, i, j)
\]

Where \( N = |D| \) i.e. is the number of ISP domains

Also from Eq. 4.10,

\[
f_i(a, b, i, j) = f_i(a, b, j, i)
\]

Hence we can say that:

\[
F_i(a, b, j) = F_j(a, b, i)
\]
Thus,
\[ K_m(MC_{a,i}, MR_{b,j}) = K_m(MR_{b,j}, MC_{a,i}) \]

The pairwise key generated by the MC and the MR is symmetric in nature. For any further communication between the MRs and the MCs, they can generate the keys as described above and securely communicate between themselves using the pairwise master-key.

### 4.4.2 Authenticated key Generation between MCs

When the MCs want to communicate with each other they simply make use of the MC domain function available to each of the MC from the upper hierarchy. The nodes simply exchange their unique IDs and the IDs of the domain they belong to and generate a symmetric key among them. Let us consider a scenario below:

In the Figure 4.6, we have two MCs: \( MC_{a,i} \) and \( MC_{b,j} \) with their unique IDs \( a \) and \( b \) in their respective domains \( D_i \) and \( D_j \). The generation in each of the MCs proceeds as follows:

\( MC_{a,i} \) uses the ID=\( b \) of the \( MC_{b,j} \) for \( q \) and the home domain ID of \( MC_{b,j} \), i.e., \( j \) in place of \( x \). The polynomial is thus evaluated to generate a key which can be used for the purpose of secure communication between them. The information obtained by \( MC_{a,i} \) by evaluating the polynomial function is used as a pairwise master key with \( MC_{b,j} \) as:

\[ K_m(MC_{a,i}, MC_{b,j}) = G_{MC_{a,i}}(q, x)|_{q=b, x=j} \]
\[ = G_i(a, q, x) \]
\[ = G_i(a, b, j) \]

Similarly, \( MC_{b,j} \) evaluates the key by substituting the ID=\( a \) and the domain address of \( MC_{a,i} \), i.e., \( i \) in
its federated domain function $G_j(b, q, x)$ in place of $q$ and $x$ respectively. The pair wise master key obtained by $MC_{b,j}$ with $MC_{a,i}$ is evaluated as follows:

\[ K_m(MC_{b,j}, MC_{a,i}) = G_{MC_{b,j}}(q, x)|_{q=a, x=i} \]

\[ = G_j(b, q, x)|_{q=a, x=i} \]

\[ = G_j(b, a, i) \]

**Proof of symmetry:**

From Eq. 4.12, we have

\[ G_i(a, b, j) = \sum_{k=1}^{N} g_k(a, b, j, i) \]

and

\[ G_j(b, a, i) = \sum_{k=1}^{N} g_k(b, a, i, j) \]

Where $N=|D|$ i.e. is the number of ISP domains

Also from Eq. 4.5 and Eq. 4.6, we have

\[ g_k(a, b, i, j) = g_k(b, a, i, j), \text{ and} \]

\[ g_k(a, b, j, i) = g_k(a, b, j, i) \]

Hence we can say that,

\[ G_i(a, b, j) = G_j(b, a, i) \]

Thus,

\[ K_m(MC_{a,i}, MC_{b,j}) = K_m(MC_{b,j}, MC_{a,i}) \]

The pair wise key generated by the two MCs is symmetric. For any further communication between the MCs, each could generate the key individually as described above and securely communicate between themselves using the pairwise master key.

### 4.5 Pairwise Session Key Generation

Once any two entities A and B (may be two MCs or a MC and a MR) in the federated WMN receive the pairwise master key, the key can be further used to derive pairwise session keys for the unicast communication between the participants of the network. A simple challenge response style protocol can be used for generating a pairwise Session key ($K_s$). Figure 4.7 above shows a challenge- response scheme designed for the secure generation of a pairwise session key ($K_s$).

**Challenge (A $\rightarrow$ B):**

Node A (MC or MR) may send a challenge to node B (MC or MR), as shown in Figure 4.7. The message consists of
Figure 4.7: Pairwise Session key generation

\[
\{A, AAA_A, E_{K_{m(A,B)}}(nonce_A), FrameNumber, B, AAA_B\},
\]

where

\(A, B\) is the ID of node A and node B respectively.

\(AAA_A, AAA_B\) represents the ID of home domain AAA of A and AAA of B respectively.

\(E_{K_{m(A,B)}}(nonce_A)\) is a random number created by node A and then encrypted with pairwise master key \(E_{K_{m(A,B)}}\).

\(FrameNumber\) is used as a timestamp, an auto-increase message count to ensure that the message received is new and thus to prevent the replay attack. Whenever any of the nodes receive the message they check the \(FrameNumber\) to determine if it is a legitimate timestamp to find the age of the message. If an old or repeating timestamp is found the message is simply dropped.

**Response (B→A):**

On receiving a challenge from node A, node B sends a response message back. The response message consists of the following fields,

\[
\{B, AAA_B, E_{K_{m(A,B)}}(nonce_B), FrameNumber, A, AAA_A\}
\]

Here, \((nonce_B)\) is the random number generated by node B, and \(E_{K_{m(A,B)}}(nonce_B)\) is encrypted with pairwise master key \(E_{K_{m(A,B)}}\).

On exchange of the challenge-response message both node A and node B decrypt the message and obtain \(nonce_A\) and \(nonce_B\). Using this information the nodes compute the pairwise session key, \(PSK (A, B)\) as

\[
K_s(A, B) = H(A, B, nonce_A, nonce_B)
\]

where, \(H()\) is the key hashing function such as HMAC or CMAC [15].
Chapter 5

Security and performance of HMSF-AKE

5.1 Security properties of HMSF-AKE

As discussed in Chapter 3, the proposed HMSF-AKE fulfills all the basic security requirements. In WMN model, the nodes belong to different level of the hierarchy. HMSF-AKE provides mutual authentication between both equal and unequal parties where not only the MRs can authenticate the MCs, but also the MCs trusts only those MRs which can generate a shared session key after the master key is generated. Specially, the mutual authentication is implemented by using the key generating domain functions, i.e., $F_{MR}$ and $F_{MC}$ for the MR-MC AKE, and $G_{MC}$ for the MC-MC AKE. In the HMSF-AKE the AAA servers in the initial phase starts o by sharing their polynomial with each other to generate a federated function. This distributed implementation assures that none of them have complete knowledge of the original polynomial that is generated originally. Furthermore, the home AAA will assign the MRs and MCs with the functions for key generation by using their IDs. As a result of this, the MR and the MC will not have knowledge of the original functions. In the pairwise master key generation phase, the home domain AAA server authenticates and assigns the functions for key generation to MCs and MRs. Only these nodes are then capable of generating a pairwise secret key. Hence, by using the trust relationship of AAA server, the MR and MC can authenticate each other.

Apart from the above, the HMSF-AKE also possesses the following properties.

- **Forward secrecy**: The node joining the network is not capable of determining any key used in the network before it joins the network.
• **Backward secrecy:** Once the node leaves the group, it is not capable of computing the key that could be used in the network.

• **Key independence:** Each of the AAAs reside in their own individual domain and generate individual domain functions, \( f_i() \) and \( g_i() \). No other AAA has any information about the function from other AAAs. For instance, if AAA\_i has function \( f_i() \) and AAA\_j has function \( f_j() \), they do not share this information. The functions are exchanged to generate the federated function \( F_i \) and \( F_j \) in the respective AAAs which is just the polynomial sum of functions generated from all other AAAs. Moreover, each AAA has its own unique ID.

• **Anti DOS attack:** HMSF-AKE is observed to be an efficient method for authentication. Every time authentication needs to be performed, the information does not need to traverse the network hierarchy to AAA so as to authenticate the MC. The MR-MC authentication indicates whether the entering node is malicious or valid and hence, the DOS attack to the backbone can be avoided.

### 5.2 Security analysis

The robustness of the generated key for communication between any two entities inherits the robustness of the key generation scheme. During the Cooperative Federated function initialization and distribution process as described in Chapter 4, Eq.(4.9) and Eq.(4.12) represent the overall robustness of scheme which is inherited by the pairwise shared.

As in [11], Ananya Gupta et al. discuss t-secure polynomial at each AAA. The polynomial generated by the AAA are all t-degree polynomial and hence their linear combination as well. “T-secure” states that the attacker would be able to compute all the coefficients of Eq.(4.1) and Eq.(4.3) if more than t-polynomials are compromised or else it cannot. At any given node the attacker will know only the linear combination of the polynomials and not individual function coefficients of \( a_{i,j,m,n} v^i w^j x^m y^n \) in Eq.(4.1) and Eq.(4.3). Higher the value of t, greater will be robustness of the overall scheme.

### 5.3 Efficiency enhancement at AAAs

Gupta et.al at [11] discusses the improvement on sharing the polynomials between various Polynomial Distributors (PDs). HMSF-AKE employs a similar strategic concept and reduces the overall overhead. The number of polynomials to be exchanged between the AAAs depends upon the net size of network itself. If we have N number of AAAs, then a single AAA would exchange \((N-1)\) polynomials.
When the exchange is between all the existing AAAs a total of \( N(N - 1) \) polynomials need to be exchanged. With large \( N \), this could result in a considerable overhead in the initial phase itself. Gupta et al. [11] have provided a naïve way to reduce the communication overhead by selecting sparse polynomial as the number of AAAs increase. Each AAA has its own individual function, \( f_i(v, w, x, y) \), whose coefficient matrix could be sparse in nature. Therefore, instead of transmitting the entire coefficient matrix, transmitting only the index values of non-zero coefficients of the sparse matrix could reduce the overall size of the message to be transmitted to the AAAs. As the number of AAA increase, the sparseness of the matrix reduces, reducing the possibilities of brute force attack by an attacker. We extend the concept in Gupta et al. [11] to see the impact of sparseness on the communication process. If \( s \) is the probability of an element in the coefficient matrix be non-zero, then \( (1 - s) \) is the probability of element in the coefficient matrix being zero. For \( N \) AAAs the probability \( p \) of an element in the coefficient matrix be non-zero is \( p = (1 - (1 - s)^N) \), where \( N \) is the number of AAAs.

As seen in Figure 5.1, as the number of AAA increase \( p \) nears 1, i.e. for small number of polynomials, the matrix is less sparse whilst it becomes increasingly sparse as the number of AAA increases.
5.4 Computational overhead and Latency performance Evaluation

One of the major communications overhead is the initial phase during the Cooperative Federated function initialization and distribution phase. As described in Section 5.3 use of sparse coefficient matrices could be one of the effective alternatives. Moreover, the exchange takes place over the hardwired IGWs and the bandwidth is of no major issue here. The communication overhead is much improved in the HMSF-AKE scheme as compared to the traditional HLR-VLR scheme of Global System for Mobile Communication (GSM). The overall time for authentication is drastically reduced in HMSF-AKE scheme as the authentication process does not need to traverse to the AAA servers all the time. The authentication is taken care of at the lower level with a 4-way handshake between any two entities (such as between MR and MC or between two MCs) one hop away.

As in any communication system, latency is very important metric in HMSF-AKE scheme. With WMNs involved in communication of real time applications such as VoIP, QoS is of utmost importance. In the proposed scheme the latency involves a 4-way handshake between two entities (between MR and MC or between two MCs) during the authentication process.

In order to evaluate the authentication delay, we perform an extensive simulation of the network model using Qualnet 4.5. We set up WMN as shown in Figure 1.1. The network comprises of two domains D₁ and D₂. The domains may be operated either by the same ISP or different ISPs. D₁ further consists of AAA₁ which is the authentication, authorization and accounting server for all other entities in D₁. D₁ also has two IGWs, IGW₁ and IGW₂, responsible for MR₁-₅ along with some random MCs. Similarly, the other domain D₂ has AAA₂ as its authentication, authorization and accounting server, IGW₃ as its internet gateway which takes care of MR₆-₉ and some MCs along.

5.4.1 Simulation Details

Simulation is performed by making use of Qualnet 4.5 simulator. Qualnet supports wide range of protocols and features specifically for the wireless networks. The network is set up as in Figure 1.1. The nodes are randomly deployed with terrain dimensions 2500 by 2500 units square in a grid type layout. Characteristics of each node are modified to meet the requirements of AAA, IGW, MR and MC design. The mobility feature has been enabled for the MC to roam between different domains.

Qualnet provides a GUI for the change in variables associated with the node. The underlying MAC protocol is 802.11s, employed in multi hop wireless connectivity [18] with 2.4 GHz frequency with 802.11b as the physical layer protocol. The routing protocol used the Hybrid Wireless Mesh Protocol (HWMP) which
is the default path protocol for 802.11s. HWMP takes most of its feature from AODV. However instead of using the hop-counts, it makes use of the radio aware metrics [19]. The mobility of the MCs is simulated by using the flag points. The flag points navigate the MCs. By maintaining the simulation time and the distance between the flags, the desired speed for the client can be achieved. As mentioned before, the AAA servers stay at the top most level. The network is simulated by placing the servers in the same or different subnets to provide an intra and inter network domain authentication. The AAA servers have 10 Mbps hard wired links between them. The network considered consists of MRs and mobile MCs. The network model is simulated with two changing factors

1. Hop count, and
2. Traffic rates.

Different hop count is simulated by adding extra nodes at the bottom of the hierarchy and in between the MRs and randomly deployed MCs. Traffic is generated using a CBR traffic generator. The rates are controlled by the simulation period and the number of packets to be sent for that period, which determines the interval time for each consecutive packet to be sent in the network. We consider each packet to be 512 bytes in size. For example, in order to generate 1Mbps of traffic, we have:

\[ 1 \text{ Mbps} = \frac{1024 \times 1024}{8} = 256 \text{ packets/sec}. \]

Now,

\[ (\text{Number of packets/sec}) \times \text{simulation time} = 256 \times 150 = 38400. \]

We have,

- \( \text{packet size} = 512, \text{interval} = \frac{1}{256} = 3.9 \text{ ms}. \text{Thus}, \)
- \( \text{Start time} = 40 \text{s and End time} = 190 \text{s}. \)

Here, we compare our proposed HMSF-AKE scheme with the HLR-VLR method, where the visiting MC needs to send information back to its home domain before the authentication can take place and thereafter, the node could join the network [16],[17]. There two different types of scenarios in HLR-VLR that we can consider.

1. Intra domain MR-MC AKE, and
2. Inter domain MR-MC AKE
In Intra domain MR-MC AKE, the MC resides only in its home domain and does not visit any other neighboring domains around it. For a MC in domain $D_1$, it would be registered with $AAA_1$, which has all its information such as ID, account name and so on. Every time MC wants to communicate, it checks with $AAA_1$ and then initiates the process. This MC always roam within the same domain. For example, in the network in Figure 1.1 $MC_1$ roams from $MR_3$ to $MR_5$. Here, both $MR_{3-4}$ and $MC_1$ belong to the same domain $D_1$ operated by the same ISP$_1$, and hence the information can be obtained directly from $AAA_1$. However, in the case of Inter domain MR-MC AKE, it is not necessary for the MC to be restricted within the same domain. In the same scenario as above when $MC_1$ moves away from its home domain $D_1$, operated by ISP$_1$ to other domain $D_2$, operated by ISP$_2$, it is said that the $MC_1$ now is in the visitor location. Before $MC_1$ could initiate any communication in $D_2$, it needs to identify itself to $AAA_2$. In this process $AAA_2$ gathers all required information from $MC_1$, verifies it with $AAA_1$ on the y and only then allows $MC_1$ to be a part of the network.

Table 5.1 provides an overview of latency involved in both Inter and Intra domain communication with multiple hops and for various traffic rates.

First we compare the Intra and Inter domain HLR-VLR scheme in terms of number of hops the MR is way from the IGW. As shown in the Table 5.1 as the distance between the MR and IGW increases so does the communication time. The overhead is less for Intra domain as compared to Inter domain as the information in Intra domain remains is localized within the same domain. However, the communication overhead is more in the case of Inter domain as the authentication servers need to exchange information between each other and pass it back to the MC.

<table>
<thead>
<tr>
<th>Hops</th>
<th>Latency (Intra Domain)</th>
<th>Latency (Inter Domain)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1hop</td>
<td>0.175</td>
<td>0.225</td>
</tr>
<tr>
<td>2hop</td>
<td>0.2105</td>
<td>0.301</td>
</tr>
<tr>
<td>3hop</td>
<td>0.2965</td>
<td>0.3605</td>
</tr>
<tr>
<td>4hop</td>
<td>0.320</td>
<td>0.5125</td>
</tr>
<tr>
<td>5hop</td>
<td>0.402</td>
<td>0.657</td>
</tr>
</tbody>
</table>
Second, shows the latency involved with different ongoing traffic rates in the network. As the traffic rate goes up, we can see an increase in the authentication latency.

<table>
<thead>
<tr>
<th>Rate (Mbps)</th>
<th>Latency (Intra Domain)</th>
<th>Latency (Inter Domain)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.7 s</td>
<td>0.8 s</td>
</tr>
<tr>
<td>3</td>
<td>0.795 s</td>
<td>0.825 s</td>
</tr>
<tr>
<td>5</td>
<td>0.78 s</td>
<td>0.83 s</td>
</tr>
<tr>
<td>7</td>
<td>0.79 s</td>
<td>0.83 s</td>
</tr>
<tr>
<td>10</td>
<td>0.825 s</td>
<td>0.86 s</td>
</tr>
</tbody>
</table>
In the proposed HMSF-AKE scheme, the authentication is resolved at a much lower level. As discussed earlier, once the function has been distributed among all the entities in the network, the authentication is involved only between the MC and the accessed MR. As we see from the Table 5.3, there is not much difference in the authentication delay as MC and MR are only a hop away and the distance between MR-IGW hops does play any role in it. The average time is 13.2 ms which could meet the QoS requirement in most of the real time application. Further, we also compare the HMSF-AKE scheme with the HLR-VLR AKES.

Table 5.3: 4 way handshakes between the Mesh Client and Mesh Router for HMSF-AKES Scheme

<table>
<thead>
<tr>
<th>Request</th>
<th>Time (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>0.016</td>
</tr>
<tr>
<td>2nd</td>
<td>0.014</td>
</tr>
<tr>
<td>3rd</td>
<td>0.02</td>
</tr>
<tr>
<td>4th</td>
<td>0.012</td>
</tr>
<tr>
<td>5th</td>
<td>0.04</td>
</tr>
</tbody>
</table>
Figure 5.4: Proposed HMSF-AKES scheme against HLR-VLR Scheme for varying no. of hops
Figure 5.5: Proposed HMSF-AKES scheme against HLR-VLR Scheme for varying traffic
Chapter 6

Conclusions and Future Work

6.1 Conclusion

HMSF-AKE scheme provides a naive and simple approach to maintain security in a WMN. With WMNs gaining popularity for real time application, it is necessary to maintain the QoS requirements as well. The scheme described in this thesis, meets the QoS benchmark. Our scheme first starts by generating and distributing the symmetric functions to MRs and MCs. The function received by each entity is unique and independent of each other, as it is evaluated using distinct IDs the node is assigned. In this process, we describe the technique that could significantly reduce the overhead, depending on the number of AAAs. We analyze the security and performance of the scheme and finally compare it with the HLR-VLR Authentication scheme. The HMSF-AKE scheme provides a fast and mutual authentication method between any two MCs and between MRs and mobile MCs in a WMN, guaranteeing a seamless handover of MCs in both inter-domain and intra-domain communication.

6.2 Future Work

Security in a communication system has always been an important issue. With more hand held devices and various other client gaining popularity, security in these devices has become a must. HMSF-AKE follows the principle of Asymmetric Key Cryptography, due to the resource constraints on MCs. Our future work could be to gain enhanced security in the network as discussed earlier. Multiple level of authentication between the MCs, also between any two MRs or MR-IGW pair can be employed. Any existing MR should be capable of authenticating any other incoming MR in the network. Additional, authentication between MR and the IGW could be employed, before MR could utilize
any of the resources. Another important work would be to add a session timestamp between any two communicating entities in order to prevent the network from replay attacks. Using the timestamp feature would allow the various entities to communicate during specific time and hence would not allow any attacker to replay the same message to gain the control of the network. With authentication at various levels, AAA-IGW, IGW-MR and MR-MR the authentication and robustness of the security can gain further enhancement.
Bibliography


