An Efficient Authenticated Key Establishment Scheme for Wireless Mesh Networks

Bing He, Saugat Joshi, Dharma P. Agrawal
Department of Computer Science,
University of Cincinnati, Cincinnati, OH 45221
Email: {heb, joshist, dpa}@cs.uc.edu

Dongmei Sun
Institute of Information Science,
Beijing Jitotong University, Beijing, China 100044
Email: dmsun@bjtu.edu.cn

Abstract—Wireless Mesh Network (WMN) is a promising technology in providing high-bandwidth Internet access over a specific coverage area, with relative lower investment cost as compared with traditional wireless access networks. Authenticated key establishment (AKE) schemes enable two entities (e.g., a client and a server) to share common communication keys in an authentic way. Due to mobility of Mesh Clients (MCs), a WMN needs to have fast and efficient AKE scheme to provide adequate security during clients handoff while meeting the Quality of Service (QoS) requirements. In this paper, we propose a lightweight distributed AKE scheme based on hierarchical multi-variable symmetric functions (HMSF). In this AKE scheme, network entities in a WMN such as MCs and mesh routers can authenticate each other and establish pairwise communication keys without any interaction from the centralized authentication center, which substantially reduces the communication overhead and authentication delay.

I. INTRODUCTION

A wireless mesh network (WMN) is a communications network consisting of wireless entities organized in an arbitrary mesh topology. In a WMN, Mesh Routers (MRs) are interconnected by wireless links and form a wireless backbone to provide ubiquitous high-speed Internet connectivity for mobile clients (MCs). The wireless backbone is tightly integrated with the Internet by a few special MRs having high speed Internet connection, which are called Internet Gateways (IGWs) [1]. WMNs not only provide high bandwidth Internet access but also offer a low cost and flexible deployment as compared to conventional access networks.

In a wireless network such as WMN, its security can more easily be compromised due to several factors [2]: distributed network architecture, the vulnerability of channels and network nodes in the shared wireless medium, and the dynamic change of network topology. Thus, an elaborate authentication mechanism is required to guarantee only legitimate users to have access to the network service. The authentication of network devices is also important for customers to ensure the authenticity of access points (e.g., MRs in a WMN) and avoid any subscription fraud. An authenticated key establishment scheme (AKES) in a WMN enables two entities (e.g., an MC and a MR, or two MCs) to share common session keys in an authentic way over open wireless links while providing mutual identity authentication between these two parties.

Several security approaches have been introduced to establish authenticated key in a wireless network. Symmetric key cryptosystems are used in mobile authentication of GSM network, and provide mutual authentications between a mobile terminal and a visited location register (VLR). However, the scheme may cause long latency in the multihop WMN. Also the scheme may suffer from denial-of-service (DoS) attacks aimed at the home location register (HLR) [3]. Public key cryptosystems also have been used for mobile authentication in wireless networks. The Extensible Authentication Protocol (EAP) is an IETF standard that provides an infrastructure for authentications between clients and authentication servers. However, most of EAP based authentication methods are quite complex and the communication and computational overheads are heavy, and lacks the ability to meet the requirements for an MC to quickly extend its ongoing session before initially authorized session expires [4]. As pointed out by Aboba [5], a quality user experience can be ensured if the latency does exceed about 50ms in VoIP or video conference, and 150ms in streaming media, while every full EAP based 802.1X authentication lead to a 1000ms latency and 250ms in fast resume mode. The authentication delay will be even worse in the multihop scenario where the authentication message will have to travel multiple hops between supplicant and authentication server. Thus, a fast and reliable authentication scheme need to be designed to meet the requirements of security and QoS in a WMN.

In this paper, a distributed authenticated key establishment scheme (AKES) is proposed based on hierarchical multi-variable symmetric functions (HMSF). The rest of the paper is organized as follows. A brief overview of the related work is provided in Section II. In Section III, the fast key establishment and mutual authentication problem is formulated on a specific WMN network model, and the symmetric/asymmetric function based key distribution methods are introduced. The detailed AKES is discussed in section IV. In Section V, the security properties and efficiency of the proposed scheme are evaluated. The conclusion of the paper is drawn in Section VI.

II. RELATED WORK

Efficient key establishment and mutual authentication is important in providing MC seamless roaming and secured access to a WMN. Khan and Akbar [6] proposed an symmetric authentication scheme for multihop WMN, which is based on EAP-TTLS (Tunneled Transport Layer Security). Fitzek et al.
[7] describe an application scheme of IEEE 802.1x in combination with UMTS-AKA to enable authentication and security in IP based multihop networks. To decrease the authentication delay, Hur et al. [4] proposed a pre-authentication scheme in a proactive way. To improve the security of authentication process in a multihop topology, Zhou et al. [8] proposed a mesh certificate based on computationally expensive public key encryption. To provide protection against DoS attack, Tang et al. [3] proposed a trust-delegation based efficient mobile authentication scheme (EMAS) based on the elliptic curve discrete logarithm problem. Lee et al. [9] proposed a distributed authentication method which is aimed at decreasing the authentication delay, in which multiple trusted nodes are distributed over the WMN to serve the role of authentication server. A solution based on the ID-based cryptography is proposed by Zhang et al [10], which features a novel user-broker-operator trust model. To provide better support for fast handover among APs maintained by multiple operators, Buttyán et al. [11] proposed two certificate-based authentication schemes. Ren et al. [12] proposed an accountable security framework with a sophisticated user privacy protection model based on a short group signature scheme.

Most of the available works are designed for wireless network with a single hop authentication. The work in this paper is motivated by Gupta et al. [13], where a decentralized key generation mechanism is proposed for cellular-based mobile ad hoc network based on shared symmetric polynomials. In this paper, we extend the conception of symmetric polynomials to a more general hierarchial hybrid symmetric functions, and apply these functions to establish authenticated keys between different entities in the WMN.

III. NETWORK MODEL AND PROBLEM BACKGROUND

A. Authenticated Key Establishment in WMN

In a large network coverage area, different service providers (e.g., ISP) provide coverage in different parts of the area, which is called mesh domains including a couple of IGWs along with attached MRs. Initially, MC will be registered to its home domain. Each ISP relies on some administrative center (e.g., AAA server) to manage different entities (such as MCs, MRs and IGWs) in its domain. Thus an ISP domain is denoted as $D_i$, which includes multiple IGWs, MRs, registered MCs, and an AAA server $AAAi$. For example, WMN in Fig. 1 consists of two ISP domains operated by $ISP_1$ and $ISP_2$. $AAAi$ is in charge of mesh domain $D_1$ of $ISP_1$, which including two IGWs and five MRs. $AAAi_2$ is in charge of one IGW and four MRs of $ISP_2$. In a federated WMN, different ISPs may decide to couple initial separated mesh domains for mutual benefit (e.g., global roaming of MCs). In this paper, we use $MR_{i,j}$ and $MC_{k,i}$ to denote a mesh router $MR_i$ mesh client $MC_{k}$ registered with home ISP $ISP_k$ respectively. We assume the connections between AAs and IGWs, between MRs and IGWs and among MRs are encrypted and secured.

The authenticated key establishment problem in a WMN discussed here includes two scenarios: AKE between MR and MC; and AKE among two MCs. The first scenario happens when a new joined MC wish to gain access to a nearby MR, or a MC moves from one MR to another MR. The inter-MCs case happens when two MCs wish to communicate with each other. A authenticated key establishment scheme for federated WMN should enable two WMN entities (MR and MC, or two MCs) authenticate each other and setup shared secret key for communication. It is also very important to reduce the authentication delay so as to provide non-interrupted service for mobile clients.

B. Symmetric Polynomial based Key Distribution Method

Polynomial based key generation scheme has been proposed by Blundo et al. [14], which is an extension of the symmetric key generation system first introduced by Blom [15]. The polynomial based key distribution scheme is a symmetric key generation system (SKGS) that an authorized server (e.g., AAA server) distributes a small piece of information (e.g., coefficients of polynomials) among a set of users in such a way that each node can compute a shared key with every other node for secure connection by only exchanging their IDs. In the scheme, each entity has a unique ID (e.g., the MAC address) which is distinct to other entities.

In a symmetric polynomial based key distribution scheme, the authenticated server generate a $k$-degree bivariate polynomial $f(x,y)$ defined as

$$f(x,y) = \sum_{i,j=0}^{k} a_{i,j} x^i y^j,$$

where the coefficients $a_{i,j} (0 \leq i, j \leq k)$ are randomly chosen from a finite field. By choosing the appropriate coefficients such as $a_{i,j} = a_{j,i}$, Eq. 1 is a symmetric bivariate polynomial with a symmetric property:

$$f(x,y) = f(y,x)$$

Figure 1. WMN Network Model

$$f(x,y) = \sum_{i,j=0}^{k} a_{i,j} x^i y^j,$$
The authentication server will assign a polynomial share \( f(i, y) = f(x, y)|_{x=i} \) to each entity \( i \) by evaluating \( f(x, y) \) at its ID \( i \), i.e., \( x = i \), thus node \( i \) has no knowledge of the original polynomial. Then, when two nodes want to communicate, they evaluate their individual polynomials with the corresponding IDs of the other to get the symmetric key. For example, node \( i \) has \( f(i, y) \) and node \( j \) has \( f(j, y) \), and would calculate \( f(i, j) \) and \( f(j, i) \) as the pairwise key respectively. Based on Eq. 2, these two quantities are equal, i.e., \( f(i, j) = f(j, i) \), and this value would be used to setup the shared symmetric key between these two nodes.

C. Asymmetric Function based Key Distribution Method

We extend the polynomial based key generation concept to the asymmetric function for mutual authentication and key establishment among a set of unequal entities. For example, in a WMN one party is MR and the other is MC. This asymmetric scheme can be used to define the type of entities. In an asymmetric function based key establishment scheme, there is a bivariate function \( f(x,y) \) which is generated by the authentication server. The first variable \( x \) is limited to entity of type A (e.g., MRs) and the second variable \( y \) is limited to the entity of type B (e.g. MC). The function can be evaluated by \( x = i \), where \( i \) is the identity of the \( MR_i \) or evaluated by \( y = j \) where \( j \) is the unique identity of \( MC_j \). The authenticated server securely transmits \( g_i(y) = f(i, y) \) to the corresponding node \( MR_i \) and \( h_j(x) = f(x, j) \) to the corresponding node \( MC_j \) respectively. Thus, nodes \( MR_i \) and \( MC_j \) has no knowledge of the original function. When two nodes wish to communicate, they evaluate their function with the corresponding IDs of the other to get the symmetric key, e.g., \( g_i(y)|_{y=j} \) in \( MR_i \) and \( h_j(x)|_{x=i} \) in \( MC_j \). Thus, \( g_i(y)|_{y=j} = h_j(x)|_{x=i} = f(i, j) \). (3) which would serve as the pairwise symmetric key between these two nodes.

IV. Hierarchical Multi-Variable Symmetric Functions basedAuthenticated Key Establishment Scheme

Based on the symmetric polynomial and asymmetric function discussed in previous section, we propose a hierarchical multi-variable symmetric function based authenticated key establishment scheme. The distributed key establishment scheme includes five procedures as follows.

A. Individual Domain Function Generation

1) Inter MR-MC Hierarchical Hybrid-Symmetric Domain Function Generation: Each AAA server \( AAA_i \) randomly generate a four variate two-level hierarchical domain function \( f_i(v, w, x, y) \) with the following symmetric property:

\[
    f_i(v, w, x, y) = f_i(v, w, x, y).
    \]  (4)

The first two variables \( v \) and \( w \) represent the MC and MR respectively. Variables \( x \) and \( y \) are to be evaluated by the ISP ID. Thus, limitations on the variables represent the hierarchical architecture of the WMN.

2) Inter MC-MC Hierarchical Symmetric Domain Function Generation: Each AAA server \( AAA_i \) also randomly generate another four variate two-level hierarchical domain function \( g_i(p, q, y, x) \), with desired symmetric property:

\[
    g_i(p, q, x, y) = g_i(q, p, x, y) = g_i(p, q, y, x). \]  (5)

The first two variables \( p \) and \( q \) represent the MCs. Variables \( x \) and \( y \) will be evaluated under the IDs of different ISPs.

B. Cooperative Federated Function Initialization and Distribution

After generating the two domain functions \( f_i(v, w, x, y) \) and \( g_i(p, q, x, y) \), \( AAA_i \) evaluates original \( f_i(v, w, x, y) \) and \( g_i(p, q, x, y) \) at \( y = j \) and securely sends two functions \( f_i(v, w, x, j) \) and \( g_i(p, q, x, j) \) to another cooperative \( AAA_j \). Thus each \( AAA_i \) can collect the functions from all cooperative AAAs and obtain the federated MC-MR function:

\[
    F_i(v, w, x) = \sum_{k=1}^{|D|} f_k(v, w, x, i), \]  (6)

where \( |D| \) is the number of federated ISP domains in the WMN.

Similarly, MC-MC federated function \( G_i(p, q, x) \) can be obtained by:

\[
    G_i(p, q, x) = \sum_{k=1}^{|D|} g_k(p, q, x, i). \]  (7)

C. Individual Function Initialization and Distribution

1) Inter MR-MC Function Initialization: When a \( AAA_i \) obtains federated function \( F_i(v, w, x) \) as shown in Eq. 6, it evaluate it using the ID of its registered customers (e.g., \( MC_{k,i} \)), as

\[
    F_{MC_{k,i}}(v, w, x) = F_i(v, w, x)|_{v=k} = F_i(k, v, x). \]  (8)

Then, it assigns this function \( F_{MC_{k,i}}(v, w, x) \) to \( MC_{k,i} \).

At the same time, each MR \( MR_{l,i} \) is given function \( F_{MR_{l,i}}(v, x) \) by \( AAA_i \) in its home domain \( D_i \):

\[
    F_{MR_{l,i}}(v, x) = F_i(v, w, x)|_{w=l} = F_i(v, l, x). \]  (9)

2) Inter MC-MC Function Initialization: Similarily, each \( MC_{k,i} \) in home domain \( D_i \) obtains the Inter-MCs function from \( AAA_i \) as below:

\[
    G_{MC_{k,i}}(q, x) = G_i(q, p, x)|_{p=k} = G_i(q, k, x). \]  (10)

D. Authenticated Pairwise Master Key Generation

1) Authenticated Key Generation between MR and MC: When MC \( MC_{a,i} \) is willing to connect to MR \( MR_{b,j} \), first they will exchange their own ID along with the ID of home domain. The MC carries the following function:

\[
    F_{MC_{a,i}}(w, x) = F_i(a, w, x). \]  (11)

Similarly, \( MR_{b,j} \) carries a function:

\[
    F_{MR_{b,j}}(v, x) = F_j(v, b, x). \]  (12)
By substituting the ID of the contacted MR \( b \) for \( w \), and the ID of the contacted MR’s home domain \( j \) for \( x \), \( MC_{a,i} \) could get the pairwise master key \( K_{pm} \) with \( MR_{b,j} \) as

\[
K_{pm}(MC_{a,i}, MR_{b,j}) = F_{MC(a,i)}(w, x)|_{w=b, x=j} = F_i(a, w, x)|_{w=b, x=j} = F_i(a, b, j).
\] (13)

Similarly, the \( MR_{b,j} \) could get the pairwise master key with \( MC_{a,i} \) as

\[
K_{pm}(MR_{b,j}, MC_{a,i}) = F_{MR(b,j)}(v, x)|_{v=a, x=i} = F_j(v, b, x)|_{v=a, x=i} = F_j(a, b, i).
\] (14)

Based on Eq. 6, we have

\[
F_i(a, b, j) = \sum_{k=1}^{\lvert D \rvert} f_k(a, b, j, i),
\] (15)

and

\[
F_j(a, b, i) = \sum_{k=1}^{\lvert D \rvert} f_k(a, b, i, j).
\] (16)

Further, from Eq. 4,

\[
f_k(a, b, i, j) = f_k(a, b, j, i),
\] (17)

which implies

\[
F_i(a, b, j) = F_j(a, b, i).
\] (18)

Thus,

\[
K_{pm}(MC_{a,i}, MR_{b,j}) = K_{pm}(MR_{b,j}, MC_{a,i}),
\]

which could be used as the pairwise master key.

2) Authenticated Key Generation Between MCs: When two MCs \( MC_{a,i} \) and \( MC_{b,j} \) plan to communicate with each other, they can simply exchange the node ID \( a \), \( b \) and home domain ID \( i \) and \( j \). Then, \( MC_{a,i} \) calculates a key by using \( MC_{b,j} \)'s ID \( b \) and corresponding AAA’s ID \( j \) with its function \( G_{MC(a,i)}(q, x) \):

\[
K_{pm}(MC_{a,i}, MC_{b,j}) = G_{MC(a,i)}(q, x)|_{q=b, x=j} = G_{MC(a,i)}(b, j) = G_i(a, b, j) = \sum_{k=1}^{\lvert D \rvert} g_k(a, b, j, i).
\] (19)

Similarly, \( MC_{b,j} \) calculates the key by using \( MC_{a,i} \)'s ID \( a \) and corresponding AAA’s ID \( i \) with its function:

\[
K_{pm}(MC_{b,j}, MC_{a,i}) = G_{MC(b,j)}(q, x)|_{q=a, x=i} = G_{MC(b,j)}(a, i) = G_j(b, a, i) = \sum_{k=1}^{\lvert D \rvert} g_k(b, a, i, j).
\] (20)

Based on Eq. 5, we have

\[
g_k(a, b, i, j) = g_k(a, b, j, i) = g_k(b, a, i, j),
\] (21)

then

\[
K_{pm}(MC_{a,i}, MC_{b,j}) = K_{pm}(MC_{b,j}, MC_{a,i}) = \sum_{k=1}^{\lvert D \rvert} g_k(a, b, i, j),
\] (22)

which would be used as the pairwise master key.

E. Pairwise Session Key Generation

Based on the above steps, two entities \( A \) and \( B \) in the federated WMN (e.g., two MCs or an MR and an MC) could get the shared pairwise master key \( K_{pm}(A, B) \). Based on the \( K_{pm} \), a pairwise session key \( K_{ps} \) could be further derived to protect communications between the two participants.

V. SECURITY PROPERTIES AND EFFICIENCY OF HMSF-AKES

A. Security Properties of HMSF-AKES

In the proposed HMSF-AKES, by exchanging IDs, only entities (MRs or MCs) that are authenticated and assigned the key generation functions by their home AAAs are able to generate the pairwise secret key. In this way, MC and MR could authenticate each other based on the trust relationship between their home AAAs.

The security robustness of the pairwise keys primarily depends on the selecting of the pairwise master key generation functions given by Eq. (6) and (7). As discussed by Gupta et. al [13], if the function is chosen based on the polynomial with \( t \)-degree, the polynomial based key distribution scheme would be “\( t \)-secure” to nodes collusion attack, which means it is secure under collusion up to \( t \) nodes. In the polynomial case, the robustness of the security key could be improved by increasing \( t \). Actually, the proposed HMSF-AKES is not limited to the symmetric polynomials, and each AAA can select more complex multi-variable symmetric functions to increase the security.

In the proposed scheme, since each mesh access point (i.e., MRs) should immediately judge whether the authentication message are from a valid or malicious clients, and the authentication are all local, thus the DoS attack to the mesh backbone could be avoided. Individual AAAs select the domain key generation functions (i.e., \( f_i() \) and \( g_i() \)) independently, which provide independence of the functions.

B. Computational Overhead and Latency Performance Evaluation

First, the storage of the multi-variable function based key materials are acceptable, especially when polynomials are used where only the coefficients of the polynomials should be stored in network nodes (MR and MC). For example, if there are \( n \) cooperated ISP domains, then there will be total \( n \times (n - 1) \) polynomials transmissions. Use of sparse matrices is also an solutions to decrease the communication and storage overhead of coefficients [13]. Computation overhead of HMSF-AKES depends on the evaluation of the function, and is usually reasonable as compared to the public key encryption.
In the proposed scheme, the communication overhead and latency are much more reduced as compared to the HLR-VLR based scheme in GSM or the EAP scheme since only one hop authentication messages exchange between two participants are required. To evaluate the authentication and key establishment delay, we perform the simulation using QualNet 4.5 simulator. The WMN consists of two ISP domains $D_1$ and $D_2$, as shown in Fig. 1. The connection between $AA_1$ and $AA_2$, and IGW and AAAs, are wired broadband link of 100Mbps. The wireless links are based on the 802.11b MAC with a maximum data rate of 11Mbps at frequency 2.4GHZ. The evaluation index is the authentication delay (in milliseconds). We compare proposed HMSF-AKE with the VLR-HLR based authentication scheme, where key materials from a visiting MC are sent back to its home AAA server through the visiting AAA via multiple hops to get the authentication[16].

Based on the relationship between the MC and accessing domain, the VLR-HLR style authentication could be classified into Intra-domain MR-MC AKE and Inter-domain MR-MC AKE. Intra-domain MR-MC AKE happens when MC is accessing an MR which belong to the same ISP domain, in which the authentication information could be got from their home AAA directly. Inter-domain MR-MC AKE happens when a MC roams between MRs which belong to different ISP domains.

First we evaluate the authentication delay when distance between the accessed MR to the associated IGW is varying from 1 to 5 hops. Each simulation is run 10 times to get the average results. As shown in Fig. 2, when the distance between accessed MR and IGW increases, the authentication delay in the VLR-HLR scheme will increase substantially. While in the proposed HMSF-AKES, the authentication and key exchange only happen between the MC and accessed MR, thus the delay will remain a constant small value of 13.2ms, which meets the QoS requirements of most real time applications. Our simulation further illustrated that when the ongoing traffic between the accessed MR and associated IGW (which are set to 4 hops away) increases from 3Mbps to 9Mbps, the authentication latency in the HLR-VLR scheme will become even worse (with a average authentication delay around 800ms) while the proposed HMSF-AKES still maintains an allowable delay less than 50ms.

VI. Conclusion

In this paper, an efficient authenticated key establishment scheme based on the hierarchical multi-variable symmetric functions is proposed for a federated multi-hop WMN. The scheme enables a fast mutual authentication and pairwise key agreement between entities in a WMN, which guarantee a seamless MC handoff among difference ISP domains. The security analysis and performance evaluation demonstrate the effectiveness and efficiency of the proposed scheme.

REFERENCES