UNIVERSITÉ DE NGAOUNDERE

Faculté des Sciences

Département de Mathématiques

Et Informatique

THE UNIVERSITY OF NGAOUNDERE

Faculty of Science

Department of Mathematics

And Computer Science

Article 12:

Duygu Karaoglan Altop, Muhammed Ali Bingol, Albert Levi, Erkay Savas: DKEM: Secure and Efficient Distributed Key Establishment Protocol for Wireless Mesh Networks. Ad Hoc Networks, 2016

By

Yera Pagore Athanase **08M521FS**

Tala Kuate Cédric **16B086FS**

Directed by

Dr. – Ing Franklin Tchakounté

Academic year: 2016-2017

Table of content

1. Introduction

1.1 Context

A computer network is define as a set of computer and peripheral interconnected in the aim to share information and resources. As the computers and many peripheral become more and more portable, the wireless network are most often implemented to use that mobility characteristic of the network components, particularly wireless mesh networks. What is concretely is wireless mesh network? A wireless mesh network can simply be define as a network based on the radio frequency, in which the exchanges are done using wireless medium through multihop mesh routing. The wireless mesh network is made up of mesh routers that are stationary, they constitute the backbone of the network, they are routing devices or access point and mesh clients which can be either stationary or mobile such as laptop, mobile phone, PDA, tablets. To increase the network's coverage, they clients collaborate to relay the information sent by the other nodes. Clients have the characteristic to be mobile compare to mesh routers, but are also more limited in energy than mesh routers. Due to that energy consumption constraints, the functionalities that require high computational power and bandwidth can be assigned to the mesh routers. Wireless mesh networks have the characteristic to be dynamically self-organized, self-configured self-healing, flexible, robust and scalable. Their advantage is that they offer both low cost and high-speed network services to end users. They can also be easily deployed even in rough and challenging terrains. The wireless nature of the transmission channel in a wireless mesh network makes it vulnerable to both passive and actives attacks. That is why it is crucial and imperative to implement a security mechanism to insure the confidentiality and the integrity of the exchanges. To achieve this security concern, a key establishment service must be provided by implementing asymmetric cryptography. Some cryptographic techniques like the Identity-base Cryptography (IBC) in conjunction with Elliptic Curve Cryptography (ECC) have been successfully used for the security issue. What can be consider as a problem with that technique is that it assume the existence of a trusted third party (TTP), responsible of the generation and distribution of the users' private keys. The disadvantage of using a trusted third party in a security protocol is that such a system will be prone to single point of failures what is neither rational nor practical. Regarding the plug and play nature of wireless mesh networks, security should be guarantee dynamically. The intervention of such a trusted third party must be avoid. In this paper submitted to our study, a

secure and efficient key establishment protocol (Distributed Key Establishment for Mesh Networks (DKEM)) is designed to handle the unique characteristics of wireless mesh networks.

1.2 Background

The (Distributed Key Establishment for Mesh Networks (DKEM)) proposed in this paper have been painted on the Identity-base Cryptography (IBC) and Elliptic Curve Cryptography (ECC). IBC eliminates the certificate-based public key distribution and ECC provides a similar level of security with RSA (Rivest Shamir Adleman) for much smaller keys sizes. RSA is an encryption system based on the difficulty of factoring very large numbers Here, two keys are used to encrypt and decrypt the information within which on is private. . The reason of this proposed solution is the use of a trusted third party in the EC-IBC, which is not appropriate due the nature of a wireless mesh network. The proposed protocol in this work is based on the proposal of Deng et al [28] described in details in the paper under the name 'the baseline protocol'.

1.3 Problem and research questions

The problem that lead the proposed solution of this paper is the assumption of the existence of a trusted third party used in the Identity-base Cryptography (IBC) in conjunction with Elliptic Curve Cryptography (ECC), by whom the users' private keys are generated and distributed for their authentication and connection to the wireless mesh network. The reason is that, using a trusted third party will make the network be susceptible to single point failure, what is not compatible with the fact that a wireless mesh network is dynamically self-organized, self-configured and self-healing, which means that the network operates in a plug-and-pay manner. The questions that have been raised by this problem are:

- How to design a secure and efficient key establishment protocol that take into account the unique characteristics of wireless mesh networks?
- How to decrease the communication and computational complexity of the existing solution?
- How to overcome the use of a trusted third party?

2. Related works

The solution proposed in this paper have been elaborated by the help of many other works dealing with the security of communication in a wireless mesh network. The most important within them are presented in a comparative form in the table below.

works	Proposed schemes	Technical approach	Applicable to WMN
[13, 14,15]	Key establishment based on the basic Diffie- Hellman (DH) key exchange protocol	Explain in [16], the exchanged random values are bind to the identities of the communicating parties	no
[17],	Mechanism based on the multi-linear DH key exchange protocol.	Explain in [18], the exchanged random values are bind to the identities of the communicating parties	no
[19],[20]	ECC	Mutual authentication of nodes with each other	no
[21]	ISA protocol	Utilize EC-IBC to solve secure key management problem	no
[22]	Key establishment protocol based on the conventional public key	A group of nodes share the role of the certification authority using ThSS	no
[23]	Similar to [22]	RSA certificate signing key is distributed among al the nodes of the network	no
[24]	Similar to [22], [23]	The private key of the central authority, assumed in ECC construction is distributed among a group of nodes	no
[25]	Use FHSS and jammer	Use FHSS to establish a secrete key in the presence of a jammer	yes
[26]	Similar to [25]	Utilize FHSS for the establishment of the shared keys by exploiting channel diversity to create link keys for the neighbors of the nodes.	Yes
[27]	Usage of one randomly selected channel node.	One of the communication nodes stays on a randomly selected channel, while the other continuously selects channels and transmits a pre-key information until the corresponding channels match.	Yes
[4,28,29]	Utilization of secret sharing	EC-IBC are used together with ThSS to manage the cryptographic keys within wireless ad hoc networks.	yes

3. Methodology employed

In this paper, the authors present a comprehensive survey of a secure and efficient key establishment protocol (Distributed Key Establishment for Mesh Networks (DKEM)). To achieve their work, they did study of the proposed and used solutions. After they did a comparative study of these existing solutions (the Baseline protocol for instance) based on respect or not of the security problem due to the plug-and-play character of the wireless mesh network. The methodology employed here is a qualitative method. The authors' interest is to gain a rich and complex understanding of the existing solution for a secure and efficient key establishment protocol (Distributed Key Establishment for Mesh Networks (DKEM)) in the aim to propose a suitable way or solution to that issue that take into account the unique characteristics of wireless mesh networks.

According to the nature of the study, a descriptive and analytical methods are used because the authors did a description of the existing solutions dealing with secure and efficient key establishment protocol (Distributed Key Establishment for Mesh Networks (DKEM)) and they also make an analysis of these solutions (Baseline protocol for instance) in the aim to compare them on some specific bases like security, resilience,

According to the purpose of the study, the methodology employed can be classified as applied research because the solution proposed is a security system which is better than the one in use. The authors also use experimentation because performed simulative performance evaluation order to show the effect of both the threshold value and the network size, which is the total number of nodes, on the latency of key establishment and on the success percentage of user private key generation, communication, computational and energy overhead.

4. Results found and Perspectives

The result presented in this paper is an efficient and secure key establishment protocol that is designed especially for wireless mesh networks. This protocol is based on identity based key establishment, but it doesn't include the usage of a trusted authority for private key generation. This task of generating a private key is achieved by the collaboration of mesh nodes. It is done as follows: a number of users exceeding a certain threshold form a coalition to generate private keys for the network users.

The authors also explored the security of both baseline and DKEM. It results to this analysis that the baseline protocol is not secure against an insider semi-honest attacker by showing how an adversary can easily obtain the master private shares of the nodes and more vitally can capture the master private key of the system. They prove that the DKEM is secure against both outsider and semi-honest insider adversaries in which the success probability of the attacker is only negligible.

According to the performance, the results show that when the size of the network increase both the latency of key establishment and the success percentage of user private key generation. For example, at the threshold value of 8, an increase in the number of mesh nodes from 40 to 100 results in 5% increase in the successful user private key generation rate and 129% increase in the elapsed time.

The results of the simulation of the baseline protocol show that DKEM outperforms the baseline protocol when either latency of key establishment, success percentage of user private key generation or network resiliency is of concern. All these results lead to the conclusion that DKEM is much efficient than the baseline protocol in all performance metrics.

The methodology used by the DKEM is also presented. It consists of three phases:

1. The master private key share generation phase
2. The master private key share distribution phase
3. The user private key generation phase

Are also presented the three different algorithms used during these phases:

Algorithm 1: is the Master Private Key share generation

```
1:procedure Phase 1: Mesh Router M_i (m, x, k)
2: for all z ∈ {1, ..., x} do
3:         select t_{i,z} & f_{i,z} (a)
4:         for all j ∈ {1, ..., m} do
5:         compute σ j, i, z
6:         if j = i then
7:                 transmit σ_{j,i,z} to M_j
8:         end if
9:         end for
10: end for
11: if ((m − 1) × x) σ_{i,j,z} 's received then
12: for all z ∈ {1, ..., x} do
13: compute γ_{i,z}
14:end for
15: broadcast FINISH
16: end if
17:end procedure
```

Algorithm 2: is the Master Private Key share distribution

```
1: procedure Phase 2: Mesh Router M_j (x)
2:      if share request by C_i & γ_{i,x} is computed then
3:          transmit a contribution reply to C_I
4:      else if share request by C i then
5:          save request
6:      else if contribution required by C_i then
7: compute ρ_{i,j}
8: transmit ρ_{i,j} to C_i
9:      end if
10: end procedure
11: procedure Phase 2: Mesh Client C_i (x, k)
12:     l← 1
13:     if FINISH message received for the first time then
14:         broadcast share request
15:     else if y > 1 & < y & γ i, then
16:         broadcast share request
17:     else if sufficient contributions received then
18:         broadcast share request with contributors
19:     else if k ρ_{i,j} 's received then
20:         compute γ_{i,}
21:         l← l +1
22:         for all saved share requests from C_j do
23:             transmit a contribution reply to C_j
24:         end for
25:     else if share request by C_j then
26:         if l> 1 & γ i, l−1 is computed then
27:             transmit a contribution reply to C_j
28:         else
29:             save request
30:         end if
31:     else if contribution required by 14 C_j then
32:         compute ρ_{j,i}
33:         transmit ρ_{j,i} to C_j
34:     end if
35: end procedure
```

Algorithm 3: is the User Private Key generation phase

```
1: procedure Phase 3: Mesh Node U_i (x, y, k)
2:      if U_i is a mesh router then
3:          e← x
4:      else if U_i is a mesh client then
5:          e ← y
6:      end if
7:      If γ_{i,z} is computed then
8:          broadcast share request message
9:      else if sufficient contributions received then
10:         broadcast share request with
contributors
11:     else if request by U_j and γ_{i,1} is computed then
12:         transmit a contribution reply to U_j
13:     else if (k − e) Γ^u_{i,j,z} 's received then
14:         compute V_i
15:     else if contribution required with p shares then
16:     if γ_{i,z} is computed then
17:         for all z ∈{1, . . . , p} do
18:             compute Γ^u_{j,i,z}
19:             transmit Γ^u_{j,i,z} to U_j
20:         end for
21:         if additive share requested then
22:             compute Γ^m_{j,i}
23:             transmit Γ^m_{j,I}
24:         end if
25:         else
26:             save request
27:         end if
28:     end if
29: end procedure
```

5. Most important publications for this work.

The important publication used for this work are presented below:

D. Karaoglan, A. Levi, E. Savas, A distributed key establishment scheme for wireless mesh networks using identity-based cryptography, in: Proceedings of the 6th ACM Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet'10), ACM, New York, USA, 2010, pp. 11–18.

M. S. Siddiqui, C. S. Hong, Security issues in wireless mesh networks, in: Proceedings of the International Conference on Multimedia and UbiquitousEngineering, IEEE Computer Society, Washington, 2007, pp. 717–722.

I. F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: a survey,Computer Networks 47 (4) (2005) 445–487.

A. Khalili, J. Katz, W. A. Arbaugh, Toward secure key distribution in truly ad-hoc networks, in: Proceedings of the Symposium on Applications and the Internet Workshops, IEEE Computer Society, Washington, 2003, pp.342–350.

R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commununications of the ACM 21 (1978) 120–126.

Z. You, X. Xie, A novel group key agreement protocol for wireless mesh network, Computers and Electrical Engineering 37 (2) (2011) 218–239.

G. Li, An Identity-based security architecture for wireless mesh networks, in: Proceedings of the IFIP International Conference on Network and Parallel Computing Workshops, IEEE Computer Society, Washington, 2007, pp. 223–226.

L. Zhou, Z. J. Haas, Securing ad hoc networks, IEEE Network Magazine 13 (6) (1999) 24–30.

J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, Providing robust and ubiquitous security support for mobile ad-hoc networks, in: Proceedings of the International Conference on Network Protocols, IEEE Computer Society, Washington, 2001, pp. 251–260

H. Dahshan, J. Irvine, An elliptic curve distributed key management for mobile ad hoc networks, in: Proceedings of Vehicular Technology Conference, IEEE Computer Society, Washington, 2010, pp. 1–5.

P. Guo, J. Wang, X. H. Geng, J.-U. Kim, A variable threshold-value authentication architecture for wireless mesh networks, Journal of Internet Technology 15 (6) (2014) 929–935.

N. Ben Salem, J.-P. Hubaux, Securing wireless mesh networks, IEEE Wire-less Communications 13 (2) (2006) 50–55.