Distributed User Authentication in Wireless Mesh Networks

Dr. Ghassan Chaddoud*

Abstract

Wireless Mesh Networks, WMNs, are foreseen to be an alternative to LANs and last- mile access infrastructures, and they have many unique characteristics, such as ease of deployment and installation, and cost efficiency. Security is crucial for WMNs to be widely accepted as internetworking and access network technologies. Access control, as a security requirement, is one of the most important pillars that lay down the foundation for such an acceptance. We identify in this paper the criteria that should be fulfilled by a viable security solution to control access to WMNs, and specify DUA, a security scheme, that allows for mutual authentication. DUA is based on the distribution of authentication key material over many nodes in such a way that any coalition of a predetermined threshold of corrupted nodes or fewer does not compromise the security of the system. Further, the key material is never handled by a single node. In addition, DUA provides for efficiency through the use of lightweight cryptographic operations.

Keywords: Access control, distributed authentication, mutual authentication, user authentication, wireless mesh networks.

* Atomic Energy Commission, P. O. Box 6091, Damascus

1. INTRODUCTION

Wireless Mesh Networks, WMNs, are one of the most promising wireless network technologies that are foreseen to be the future of access networks. They are an alternative to LANs and last mile access infrastructures. WMNs have many unique characteristics such as ease of deployment and installation, cost efficiency, and self-organizing and self-healing capabilities.

Typically, a WMN consists of many routers, known as *mesh routers*, connected together via wireless connections, *e.g.*, 802.11, 802.15, and 802.16, to form the *mesh backbone infrastructure*, as shown in Figure 1. The mesh routers allow mesh *clients* to get access via multi-hop connections to other networks, such as the Internet, cellular phone networks, and ad hoc networks. The mesh clients can make use of the mesh backbone to connect to each other or to other networks. The connections with other networks are ensured via *mesh gateways*, which form bridges with different types of networking technologies.

Despite the fact that WMNs were the subject of many interesting research and development works, WMNs technologies are still in their cradle [1, 8], and a lot of more appropriate mechanisms related to internetworking, MAC, routing, congestion control, QoS, and security are still missing. The only work that covers most of these aspects is 802.11s [2] which is an amendment to 802.11 to handle mesh networks and it is about to be rectified. However, 802.11s security mechanisms are based on a password known to all nodes in the WMN; an attacker could impersonate any other node and hence illegally get access into the network.

In fact, security is crucial for WMNs to be widely accepted as internetworking and access network technologies. Particularly, Access control as a security requirement is one of the most important pillars that lay down the foundation for such an acceptance. It allows for WMNs' operators to control access to their services on one side, and for clients to authenticate the access network they are connecting to, on the other side. Further, access control, in particular, user authentication, allows communicating entities to share secrets and hence pave the way to ensure other security requirements to user data, such as confidentiality, integrity, and origin authentication.

Although WMNs offer the same functionality as wired and wireless access networks such as 802.11 and 802.3, their security mechanisms are not suitable for WMNs because access in these networks is based on a presumably available authentication center [3]. Further, access control mechanisms in wireless LAN [4] is not convenient for wireless multi-hop communications. Even security mechanisms in other wireless multi-hop networks, such ad hoc's and sensor's, which are independent from any other networks and their nodes belong to the same organization or are a priory known to each other, are not suitable either.

In this paper, we identify the criteria that should be fulfilled by a security solution to control access to WMNs, and specify DUA, Distributed User Authentication, as a security scheme that allows for mutual authentication. Section 2 identifies the requirements of a viable security solution. Section 3 overviews related works Section 4 describes the network and trust model we adopt in our work. Section 5 describes DUA, our approach, to ensure mutual authentication. Section 6 evaluates the impact of the proposed scheme. Section 7 is a conclusion

2. VIABLE SECUIRTY SOLUTION

Similarly to other wireless networks, Security in WMNs is of paramount importance, due to their deployment and operating environment; the wireless connection nature makes nodes unreachable in some situations. Therefore, *availability* is an important objective to be achieved by a viable security solution. One would rely on security solutions based on entities outside the WMNs, or embedded in the mesh gateways, which is much better from a security point of view, nevertheless, the network would become easily unavailable due to denial of service attacks caused by the nature of multi-hop communications which delays attack discovery. Our solution provides for availability through redundancy; authentication key material is replicated over many nodes.

Further, WMN infrastructure nodes are deployed in an unattended manner far away from any physical protection or surveillance. This makes the capture of any node with security functionalities compromises the security of the whole network. So, a viable security solution must support *fault-tolerance* so as to counter attacks aimed at tampering with those nodes, on one hand, and to not compromise authentication credentials stored within corrupted nodes, on the other hand.

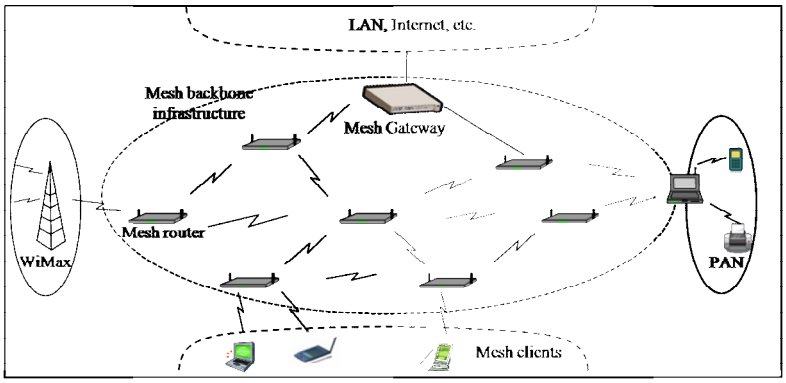

Fig. 1. A wireless mesh network which serves as a connection infrastructure to PAN and WiMax cleints,and a network access to mesh clients.

As a result, distributed solutions are more favorable over centralized ones so as to stand up to malicious attack and hence, to ensure *secrecy*. In other words, secrecy protects keying material against disclosure attacks caused by compromised nodes, while fault-tolerance stands up to authentication key material disclosure caused by a coalition of corrupted nodes. We opt for the distribution of authentication key material over many nodes in such a way that no coalition of a predetermined threshold of corrupted nodes or fewer is not able to compromise the security of the system. In addition, the key material is never handled by a single node.

Furthermore, mesh clients such as PDAs, smart phones, laptops, and the like, might be of limited capabilities or multipurpose devices, therefore any security solution must take into account these characteristics and by consequence must reduce communication, storage, and processing overhead as much as possible. And as a result the security solution must support *efficiency*.

3. RELATED WORKS

Recently, many works have focused on security threats and requirements in WMNs. [8] identified three security challenges: detection of corrupt nodes, secure multi-hop routing, and fairness caused by MAC protocols. [13] stressed on these challenges and pointed out the importance of cooperation between nodes to enforce trust in the absence of a trusted infrastructure. Inspired by [8] and based on ad hoc network threats, [14] distinguished MAC-sublayer and network layer threats. [11] detailed further the requirements and analyzed some proposed security solutions with regard to communications patterns between WMN nodes.

Regarding user authentication, proposed approaches to authenticating WMN clients can generally be classified as distributed or centralized. A distributed approach is characterized by the fact that a group of entities are responsible for authenticating clients. Usually, authentication functionalities

are distribution over many dedicated nodes, called hereafter, distributed authentication servers, DASs. TUA [5], MeCA [6], and [7] are examples of such a class. In a centralized approach, such as 802.11s [2], ARSA [9], Mobisec [10], and AKES [15] one single entity, called authentication server, handles the authentication functionalities.

TUA [5] proposes a distributed user authentication mechanism based on a (*t*, *n*) threshold scheme [12], where shares of the authentication server group's private key are distributed to *n* mesh routers, or servers, and any coalition of *t* or more servers could cooperate to generate identity-based partial signatures on a secret pre-shared between the user and a trusted third party. If the mesh access point can verify the signature reconstituted from these partial signatures then this means that the user is the one with the identity who claims and in possession of the related password. Operations in TUA are carried out within cyclic additive and elliptic curve multiplicative groups, complexity of these operations are of the order of $O(lg(n)3)$.

Similarly, MeCA [6] is based on a (*t*, *n*) threshold scheme, where certificate authority's private key is distributed as shares on *n* mesh routers and any coalition of *t* or more routers could cooperate to issue, revoke, or update certificates of mesh clients. [6] improves efficiency by reducing communication overhead through the use of multicasting trees. Further, it takes into account the changing membership of mesh routers when new routers join the group or others leave it, *i.e.*, *n* is not fixed. [7] improves on this by handling compromised shares, *i.e.*, *t* is not fixed.

802.11s [2] ensures client authentication based on a pre-shared key, known as a password. Any client who knows the password can authenticate itself to any mesh router and hence gets access to the mesh network. Therefore, [2] provides group authentication rather than entity authentication.

ARSA [9] is based on identity-based cryptography. It allows a broker to issue signed passes to mesh clients, then any mesh node that trusts that broker can verify the pass and allow the client to get access to the network. Despite the fact that ARSA is based on asymmetric cryptography, it uses identity-based cryptography. The main problem of ARSA is its incapability to deal with broker corruption.

Mobisec [10] is another centralized scheme based on [4] authentication mechanism; it allows a mesh client to authenticate itself to a key server or to any delegated router that has the client key obtained from the key server. However, the corruption of any delegated router with the right keying material will compromise the authentica-tion service.

AKES [15] allows a client and a mesh router to authenticate each other based on the knowledge of a pre-shared symmetric bivariate polynomial evaluated at their respective identities. In addition, a pairwise key is computed by both parties. AKES provides for efficiency, however, it is not resistant to compromising entities.

Generally, centralized approaches do not meet availability, fault-tolerance, and secrecy requirements because the compromise of the authentication server, or any delegated entity, exposes the whole network where this situation is inevitable in wireless environment. Yet, they remain appealing in situations where the authentication server is immune against different types of attacks, with functionalities replicated over many entities

4. SYSTEM MODEL

We explain in this section the WMN model we adopt, and the assumptions we make regarding relationships between nodes.

A. Network Model

Regarding the way networks are operated within a limited coverage area, [8] pointed out that many WMNs may coexist in the same geographical area, where each one is operated and administrated independently, or one single infrastructure is shared among many operators, *i.e.*, the same router may be exploited by more

than one operator. In other words, clients of different operators can get network access using the same access points and mesh routers. However, since securing this type of WMN application is much harder than one single WMN deployed inside a limited zone and operated by a single operator. In addition, we aim in this work to boost the use of WMNs as an extension to 802.11 LANs. So, we restrict ourselves to the case where the network is not shared among operators.

Our network model is composed of:

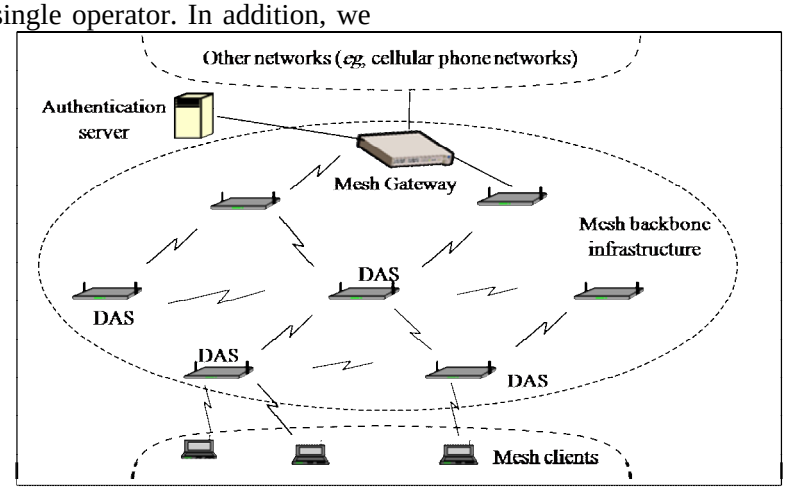

Fig. 2. WMN model. Distributed Authentication Server (DASs) authenticate clients during access session, and the Authentication Server manages client keys

- Mesh backbone infrastructure: composed of mesh routers and mesh gateways. While mesh routers are responsible for relaying data and granting network access to mesh clients, gateways ensure interfacing with the Internet or other networks, as shown in Figure 2. We assume that components of the infrastructure are stationary.
- Mesh clients: clients are one single hop away from the mesh backbone and use it to connect to each other or to other networks. Although, clients might be mobile, we assume that they are stationary during an access session.

B. Trust Model

[9] distinguished mesh infrastructure security and network access security:

- Mesh infrastructure security: concerned with the protection of the signaling and data traffic over the mesh backbone infrastructure.
- Network access security: ensures security services to communication between mesh clients and mesh routers.

Since we opted for the case where the mesh infrastructure owned and operated by one single operator; it is fair enough to assume that a trust relationship is in place among the components of the infrastructure. Further, we assume that there exist secure channels between every pair of neighbouring mesh routers, between mesh routers and neighbouring mesh gateways, and between mesh gateways and an outsider key server, referred to as *Authentication Server*, AS. Furthermore, mesh routers grant access to clients who have the correct credentials, an IDs and a client key for instance. The client key is a pairwise key shared between the client and the authentication server. The authentication server is outside the WMN and connected to gateways by either wired or wireless connections.

The client credentials are issued by the operator to clients in an offline or online

manner, *i.e.*, during user registration or client key update carried out by an appropriate mechanism. In other words, a client is regarded as a trusted and legitimate WMN client in the case she/he presents valid credentials, in particular, her/his client key.

5. DISTRIBUTED AUTHENTICATION

As mentioned earlier, a distributed approach to control access to WMNs is by far more favourable than a centralized one. Our approach to authenticate clients is based on the distribution of client credentials, in particular, client keys to *n* mesh routers, called hereafter *distributed authentication servers*, or DAS, in such a way that no coalition of *t-1* servers or fewer can reconstitute any of the authentication keys. *t* is smaller or equal to *n* (number of WMN mesh routers.

The key idea for distributing the client key is as follows: the authentication server generates for each client *i*, *t* number of keys $K_{i,j}$, and computes client *i*'s key as the XOR of these *t* keys, *i.e*.

$$K_i = K_{i,1} \oplus \ldots \oplus K_{i,t}.$$

$K_{i,j}$ are referred to as client *i*'s key shares and will be distributed to *t* DSAs participating in client authentication in such a way that when a user requests access to the WMN, the *t* DSAs holding client *i*'s shares have to cooperate to decide whether the client holds or not a valid client key, and by consequence valid credentials.

A. Setup phase

We presume that a client *i* who wants to get access to the WMN is registered with the network operator. The DASs forms a multicast group with identifier and address known to each DAS server. The group is used to address authentication requests to its members, and to distribute and update keying material.

The authentication server generates for the client *i*, an identifier ID_i and *t* key shares $K_{i,j}$, and distributes them to *t* DASs, *t* must be odd and smaller or equal to *n*. The *t* DASs might be picked up randomly from the *n* DASs. The shares are sent along the ID_i and other information to the chosen DASs using secure channels pre-established between the authentication server and DASs.

B. WMN access

We explain in this subsection how client *i* and the DAS groups authenticate each other during user join to the WMN. Figure 3 illustrates the message exchange:

– Client *i* forms an authentication request *m* and sends it to a mesh router playing the role of an access point, AP, whose identifier is ID_{ap}. The message contains client *i*'s identifier ID_i, AP's identifier ID_{ap}, WMN identifier SSID, a nonce n_i, and $AUTH\_REQ_i = CRC(c) \oplus K_i$, where $c = ID_i \,||\, ID_{ap} \,||\, SSID \,||\, n_i$, CRC is a Cyclic Redundancy Check function, and n_i is used to prove the request freshness and might be used to generate a key shared between the AP and client *i* so as to protect further communication between the AP and the client.

– The AP multicasts $AUTH\_REQ_i$ to DASs using the multicast group address.

– Every DAS server *j*, uses client *i*'s ID_i to lookup client *i*'s share $K_{i,j}$ and computes a partial authentication reply $AUTH\_REP_{i,j}$,

$$AUTH\_REP_{i,j} = AUTH\_REQ_i \oplus K_{i,j} = CRC(c) \oplus K_i \oplus K_{i,j},$$

and sends the partial reply to AP. Notice that the AP might be itself a DAS.

– Once the AP has collected the *t* partial authent-ication replies, it computes

- 1st: $AUTH\_REP_i = AUTH\_REP_{i,1} \oplus \ldots \oplus AUTH\_REP_{i,t}$
- 2nd: $r' = CRC\,(ID_i \,||\, ID_{ap} \,||\, SSID \,||\, n_i)$

Notice that

$$AUTH\_REP_{i,1} \oplus \ldots \oplus AUTH\_REP_{i,t}$$

$= \text{CRC}(c) \oplus K_i \oplus K_{i,1} \oplus ... \text{ CRC}(c) \oplus K_i \oplus K_{i,t}$,

$= \text{CRC}(c \oplus ... \oplus c) \oplus K_i \oplus \ldots \oplus K_i \oplus K_{i,1} \oplus ... \oplus K_{i,t,}$

$= \text{CRC}(c) \oplus K_i \oplus \ldots \oplus K_i \oplus K_{i,1} \oplus ... \oplus K_{i,t,}$

This is due the linearity of CRC with regard to XOR operator and t is an odd number.

Hence, $\text{AUTH\_REP}_{i,1} \oplus ... \oplus \text{AUTH\_REP}_{i,t} = \text{CRC}(c) \oplus K_i \oplus K_{i,1} \oplus ... \oplus K_{i,t} = \text{CRC}(c)$, because $K_i = K_{i,1} \oplus ... \oplus K_{i,t}$

Then, $\text{AUTH\_REP}_i = \text{CRC}(c)$

The AP considers client i as a legitimate client if $r' = \text{AUTH\_REP}_i$

– If $r' = \text{AUTH\_REP}_i$, the AP sends client i a message m' containing AUTH_REP_i, n_{ap} and in addition to ID_i, ID_{ap}, SSID, and n_i. n_{ap} plays the same role as n_i does.

– Client i computes $\text{CRC}(\text{ID}_i \| \text{ID}_{ap} \| \text{SSID} \| n_i)$ and compares it with AUTH_REP_i, if they are equal, client i considers the network as authenticated, and he proceeds further in his access process with the WMN.

C. One-time key

The precedent protocol allows for mutual authentication; the client and the WMN authenticate each other, however, the message exchange exposes the client i's key: either the AP or a snooper could obtain K_i or $K_{i,j}$ by x-oring requests and replies.

To resolves such a problem, we propose to use the client key and its shares only one time. This would be a huge task to be handled by DASs and the authentication server itself. What we propose here is to take advantage of one-way functions in such a way that we deal with the user's key and shares as master key and master shares respectively, and derive a *key chain*[1] of size d for example, of keys and shares by using a one-way function that is linear with regard to the XOR operator. A CRC[2] function is an instance of such a one-way function. Notice that d would be the number of access times the client requests access to the WMN, or represents the validity period of the key, and could be heuristic and determined by the WMN operator. For example, if the average of access times the client gets access the WMN is 5 per day and we would not use the client key for more than a week, then d could be equal to 21.

We show in the following how the one-time key K_i^f and related shares $K_{i,j}^f$ are derived from the client i's key and shares by using the CRC as a one-way function.

$K_i^0 = K_i$,

$K_i^1 = \text{CRC}(K_i)$,

$K_i^2 = \text{CRC}(K_i^1) = \text{CRC}^2(K_i)$,…

$K_i^d = \text{CRC}(K_i^{d-1}) = \text{CRC}^d(K_i)$.

In the same way each DAS holding client i's share $K_{i,j}$, creates a chain of shares as follows:

$K_{i,j}^0 = K_{i,j}$,

$K_{i,j}^1 = \text{CRC}(K_{i,j})$,

$K_{i,j}^2 = \text{CRC}(K_{i,j}^1) = \text{CRC}^2(K_{i,j})$,…

$K_{i,j}^d = \text{CRC}(K_{i,j}^{d-1}) = \text{CRC}^d(K_{i,j})$.

Now, client i who wants to get access to the WMN for the first time uses its K_i^d, second time uses K_i^{d-1}, … , the k^{th} times he uses K_i^{d-k+1}, and so on.

Similarly, client i's shareholders j, uses for the first time the share $K_{i,j}^d$, for the second time $K_{i,j}^{d-1}$, … , and for the k^{th} time $K_{i,j}^{d-k+1}$, and so on.

Notice that

[1] The Idea of the key chain is borrowed from TESLA [16].

[2] Cyclic Redundancy Check.

$$K_i^{d-k+1} = \mathrm{CRC}^{d-k}(K_i)$$
$$= \mathrm{CRC}^{d-k}(K_{i,1} \oplus \ldots \oplus K_{i,t})$$
$$= \mathrm{CRC}^{d-k}(K_{i,1}) \oplus \ldots \oplus \mathrm{CRC}^{d-k}(K_{i,t}).$$
$$= K_{i,1}^{d-k+1} \oplus \ldots \oplus K_{i,t}^{d-k+1}$$

Regarding the complexity of the use of one-time key, the one might consider that the complexity of the operations make it unattractive since every DAS and the client have to carry out *d-k+1* CRC operation during the k^{th} access, however, the number of CRC operations can be attenuated either by computing the one-time key and shares once, or by preparing the right one-time share during idle time.

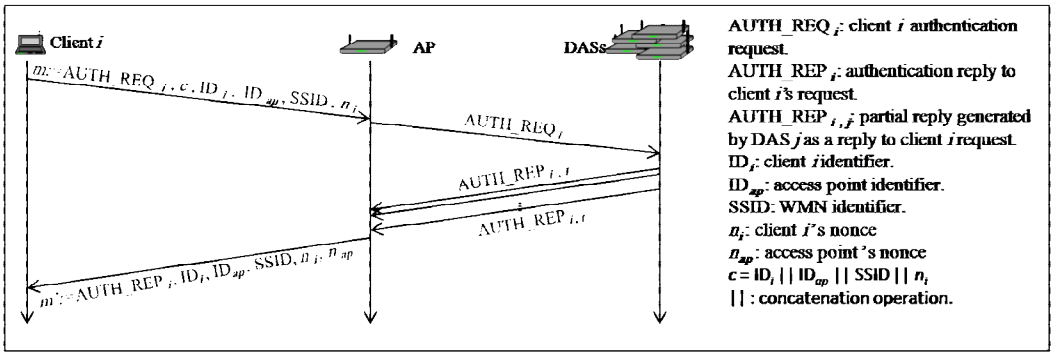

Fig. 3. DUA message exchange during client access.

D. Replicated shares

In order for our solution to work we imposed that the *t* DASs holding shares of client key must participate in the authentication process. However, this condition cannot always be met in WMNs for the reasons mentioned above. The unavailability of any DASs, and by consequence, the unavailable share held by unavailable DAS, renders the authentication process impossible to be achieved.

To overcome this problem we propose to deploy many copy of the same key share over many servers. This can be done by replicating the same share over many DASs. And every DAS must participate in the authentication process.

Since the absence of a shareholder could be caused by either a general failure (communication or hardware), or an attack that might be targeted, in the worst case, towards a region in the deployment area of the network. Therefore, we propose to divide the geographical deployment area into zones and distribute replicas of the shares to DASs situated in distant zones so as not to compromise all the copies of the same share. Notice that in such a situation compromising a set of DASs or the whole DASs in a zone would compromise a copy of a share, but not the whole copies of the same share.

If a DAS is temporally out of reach or is compromised other DASs are able to generate partial replies.

When generating partial replies every DAS that has a copy of a share sends a partial reply. The AP, when receiving multiple partial replies generated using the same share, compares them if they are equal then it uses any of them to construct the final reply. If a partial reply is different from the other partial replies, then the AP expels it and uses any of the other partial replies. If the number of received partial replies is less than the expected number of partial replies, then it is fair enough to consider that one or more DASs holding a copy of a share are out of reach. Figure 4 shows a WMN divided into 9 zones, where DAS 1, DAS 2, DAS 3, DAS4, DAS 5, DAS 8, DAS 9, and DAS10 are Distributed Authentication Servers (DASs) holding copies of client *i* key shares $K_{i,1}$, $K_{i,2}$, $K_{i,3}$, and $K_{i,4}$. Notice that if an attacker targeted Zone 2, a copy if key share $K_{i,1}$,would become compromised, however, other copies of the

same share, such as the one held by DAS 8 in zone 7, is still available.

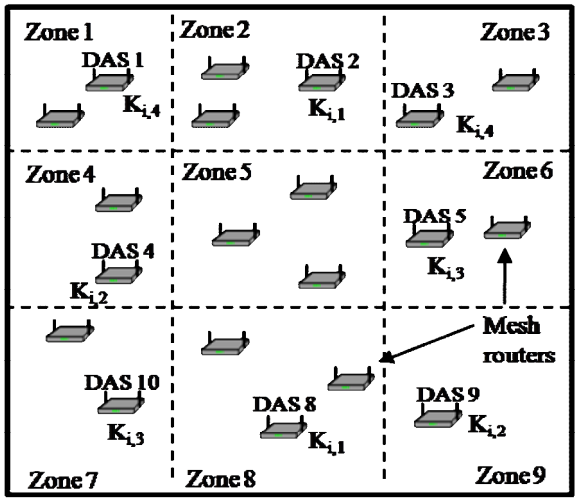

Fig. 4. A WMN divided into 9 zones, where DAS 1, DAS 2, DAS 3, DAS4, DAS 5, DAS 8, DAS 9, and DAS10 are Distributed Authentication Servers (DASs) holding copies of client *i* key shares $K_{i,1}$, $K_{i,2}$, $K_{i,3}$, and $K_{i,4}$.

6. EVALUATION AND ANALYSIS

In this section, we show how DUA fulfils the requirements of viable solution as other distributed solutions do. In addition, we prove that our solution is more efficient than the others.

Despite the fact that most of earlier distributed approaches, (*i.e.*, [5], [6], and [7]), make use of the same secret sharing scheme to ensure the requirements of viable solution: availability, fault-tolerance, and secrecy. However, since the cryptographic operations are asymmetric, so these solutions might not be suitable to mesh nodes.

Our solution fulfils the first three requirements using different mechanisms. First, secrecy is provided by partitioning client key into shares and no node is aware of the whole key, so the compromise of any DAS would not reveal any key. Second, fault-tolerance is ensured via distributing key shares to mesh routers; compromising any number of DASs fewer than t would not reveal the client key. Third, availability is fulfilled by replicating key shares over distant mesh routers.

Regarding efficiency, we compute in the following the storage, processing, and communication overhead per DAS generated by our scheme within the mesh infrastructure. We assume that, α is the redundancy factor, d is the size of the key chain, z is the size of the client key and the shares, and m is the number of clients whose keys are handled by a DAS.

If we assume that our scheme relies on multicast to send authentication requests, then the total number of messages is the number of authentication replies ($t * \alpha$), in addition to a multicast message. As for the storage overhead, we consider the case where every DAS computes the key chain for every client beforehand, then the storage data size is ($d * z$) * m. In this case the processing overhead is (d* C * m), plus a XOR operation when generating a partial authentication reply. C is a CRC operation.

As a result, our solution is more efficient than the other distributed solutions because it is mainly based on lightweight operations, such as CRC and XOR, which are much faster and easier to use than any other symmetric and asymmetric mechanisms and is more convenient to mesh clients with limited resources. In addition, CRC functions are known to be the fastest hash algorithms.

7. CONCLUSION

We proposed in this paper DUA a new scheme to control access to a WMN that serves as an access network and is operated by a single operator. The proposed access control solution fulfils the identified criteria of a viable security solution; availability, fault-tolerance, and secrecy. Further, it allows efficiently for mutual authentication between mesh clients and the WMN; since it is based on lightweight operations compared to other

cryptographic primitives.

Despite the fact that the CRC function is at the heart of our work and the security of DUA depends mainly on its cryptographic properties, any other hash functions that are linear with regard to the XOR operator could be an alternative when the security of the CRC function is questioned. In the main while, a CRC function with hash value size big enough, such as 64 bits[3], might be suitable to protect client keys with a validity period of many days.

[3] Such as CRC-64-ECMA-182.

References:

1. Akyildiz, I. F., Wang, X., and Wang, W., "Wireless mesh networks: a survey", Computer Networks, vol. 47, pp. 446–487, 2005.
2. IEEE 802.11s Task Group, Amendment: ESS Mesh Networking, D3.0.
3. 802.1X-2004 - Port Based Network Access Control, IEEE Standard.
4. IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standards.
5. Lin, X., Lu, R., Ho, P.H., Shen, X. and Cao, X., "TUA: A Novel Compromise-Resilient Authentic-ation Architecture for Wireless Mesh Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 4, April 2008.
6. Kim, J. and Bahk, S., "Design of certification authority using secret redistribution and multicast routing in wireless mesh networks", Computer Networks, vol. 53, issue 1, 2009.
7. Yang, K., Jia, X, Zhang, B. and Zhongming, Z., "Threshold Key Redistribution for Dynamic Change of Authentication Group in Wireless Mesh Networks", in Proceedings of GLOBECOM'10, 6 – 10 Dec, Miami, Fl, 2010.
8. Ben Salem, S. and Hubaux, J. P., "Securing Wireless Mesh Networks", Wireless Communica-tions, vol. 13, pp. 50 - 55, 2006
9. Zhang, Y. and Fang, Y., "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks", IEEE Journal on Selected Areas in Communications, pp. 1916 – 1928, 2006.
10. Martignon, F., Paris, S. and Capone, A., "MobiSEC: A Novel Security Architecture for Wireless Mesh Networks," in Q2SWinet, 27 – 31 Oct, Vancouver, Canada, 2008.
11. Egners, A. and Meyer, U., "Wireless Mesh Network Security: State of Affairs", in the Proceedings of 6th IEEE LCN, Danver, USA, 11- 14 Oct, 2010.
12. Desmedt, Y. and Frankel, Y., "Threshold cryptosystems", *Advances in Cryptology*, LNCS, Springer-Verlag, vol. 435, pp. 307-315, 1990.
13. Siddiqui, M. and Hong, C. S., "Security Issues in Wireless Mesh Networks," in Proceedings of *MUE' 07*, Seoul, 26 – 28 April, 2007.
14. Glass, S., Portmann, M. and Muthukkumarasamy, V., "Securing Wireless Mesh Networks," IEEE Internet Computing Special Issue on Wireless Mesh Networks, pp. 30 - 36, 2008.
15. He, B., Joshi, S., Agrawal, D.P. and Dongmei, S., "An Efficient Authenticated Key Establishment Scheme for Wireless Mesh Networks", in Proceedings of *GLOBECOM'10*, 6 – 10 Dec, Miami, Fl, 2010.
16. Perrig, A., Canetti, R., Song, D. and Tygar, D., "Efficient and Secure Source Authentication for Multicast", in Proceedings NDDS'01, San Diego, CA, Feb. 2001.

9-Glossary

Access	نفاذ
Attack	هجوم
Authentication	وثوقية، استيقان
Availability	إتاحة، وفرة
Centralized	مركزي
Client	زبون
Confidentiality	سرية
Congestion	اختناق
Control	تحكم
Cryptography	تعمية
Denial of service	حجب أو رفض خدمة
Distributed	موزع
Gateway	بوابة
Fault-tolerance	التساهل مع الأخطاء
Infrastructure	بنية تحتية
Integrity	تكاملية، سلامة
Key	مفتاح
Mechanism	آلية
Mesh	عروي
Multi-hop	متعدد القفزات
Mutual	متبادل
Network	شبكة
Node	عقدة
Operator	مشغل
Quality of Service, QoS	جودة خدمة
Redundancy	غزارة، وفرة
Requirement	متطلب
Router	موجه، مسير
Security	أمن
Server	مخدم
Service	خدمة
Threat	تهديد
Threshold Schemes	مخططات عتبية
Viable	قابل للحياة

Received 18/12/2011