Performance Evaluation of Different CRL Distribution Schemes Embedded in WMN Authentication[*]

Ahmet Onur Durahim, İsmail Fatih Yıldırım, Erkay Savaş and Albert Levi

durahim, ismailfatih, erkays, levi@sabanciuniv.edu
Sabanci University, Istanbul, Turkey

Abstract. Wireless Mesh Networks (WMNs) have emerged as a promising technology to provide low cost and scalable solutions for high speed Internet access and additional services. In hybrid WMNs, where mesh clients also act as relaying agents and form a mesh client network, it is important to provide users with an efficient anonymous and accountable authentication scheme. Accountability is required for the malicious users that are to be identified and revoked from the network access and related services. Promising revocation schemes are based on Certification Revocation Lists (CRLs). Since in hybrid WMNs mesh clients also authenticate other clients, distribution of these CRLs is an important task. In this paper, we propose and examine the performance of different distribution schemes of CRLs and analyze authentication performance in two scenarios: in one scenario all mesh routers and mesh clients obtain CRLs and in the second one, CRLs are held only by the mesh routers and mesh clients acting as relaying agents require CRL checking to be performed from the router in authenticating another client.

1 Introduction

Recently, using mobile devices and wireless networks become a convenient and inexpensive way to connect to Internet. In this respect, hybrid WMNs are proposed as a solution where mesh clients and routers collaboratively form a well-connected network. Generally, WMNs are comprised of mesh routers and mesh clients (network users), whereby mesh routers are in charge of providing coverage and routing services for mesh clients which connect to the network using laptops, PDAs, smartphones, etc. Hybrid architectures [2] (*cf.* Figure 1) are the most popular since in addition to mesh routers, mesh users may also perform routing and configuration functionalities for other users to help improve the connectivity and coverage of the network. Ubiquity and invasiveness of WMNs, however, pose serious challenges for security and privacy of individuals who cherish their benefits. Being connected via a smart mobile device may necessitate entrusting one's privacy to some - not necessarily trustworthy - third parties to varying extents. In many cases, privacy is simply ignored. As in the case of security, initial authentication of a user to the network is a key point for privacy protection. On the other

[*] Erkay Savaş, and Ahmet Onur Durahim are supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Project number 105E089. Albert Levi and İsmail Fatih Yıldırım are supported by Turk Telekom under Grant Number 3014-01.

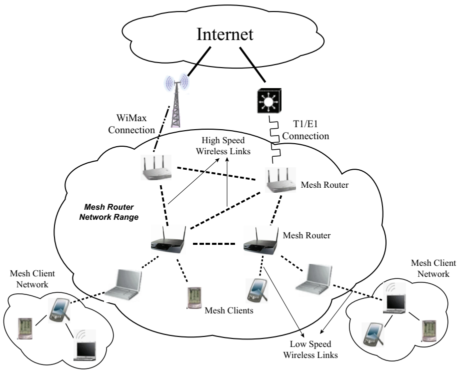

Fig. 1.: Hybrid WMN architecture

hand, uncontrolled anonymity encourages some users with ill intentions to act maliciously, since they would not be identified or tracked due to their anonymous access to the network.

Therefore, anonymous authentication frameworks to be proposed for the hybrid WMNs should both satisfy necessary privacy and accountability requirements at the same time. Revocation mechanisms play a crucial role in providing accountability by identifying and revoking a malicious user. Most promising revocation mechanisms are based on Certification Revocation Lists (CRLs), where an identifier of a network user is added to the list in order to prevent a revoked user from future access to the network. Thus, required check on deciding whether an authenticating user is revoked or legitimate, can only be performed by the entity who holds the CRL. Furthermore, this check must be accomplished with an up-to-date list. So, it is important to determine where to keep the CRLs and how to update them and where to perform the revocation check.

There are two alternative CRL distribution solutions are proposed and examined in this paper: First, CRLs are held both by mesh routers and mesh clients acting as relaying agents. In the second alternative, CRLs are held only by the mesh routers and revocation check is performed by the mesh routers on behalf of the relaying agents authenticating an another mesh clients.

In order to examine these alternatives, A^2-MAKE framework [4] is chosen as a base authentication platform where users can connect to the network in an anonymous and accountable manner and revocation mechanism in A^2-MAKE is based on the CRLs[2].

2 A^2-MAKE

A^2-MAKE framework is a collection of protocols that provides anonymous mutual authentication to its users whereby legitimate users can connect to network from anywhere without being identified or tracked unwillingly. No single party (or authority, network operator, etc.) can violate the privacy of a user. User accountability is implemented via user identification and revocation protocols where revocation is performed using CRLs.

[2] This list is named as UserRL in A^2-MAKE

In order to connect to the network in A^2-MAKE, network users authenticate themselves to the mesh routers if there is one in communication range. Otherwise, they are connected to the network by mesh clients acting as relaying agents if they find one in their communication range. If the authentication is performed by the mesh routers, routers provide their authentication payload using conventional digital signature algorithms since routers does not require privacy protection. On the other hand, relaying agents who are also mesh clients that require privacy protection provide authentication payload using anonymous authentication scheme. In both connection attempts, authenticating mesh client performs anonymous authentication procedures.

In order to provide accountability, user identification and revocation procedures are proposed, whereby an identifier is added to the UserRL to revoke a user. So, authenticating agent checks this list in order to determine whether a network user is a legitimate or a revoked one.

3 CRL Distribution Scenarios

We propose two different CRL distribution scenarios, based on where the list is held which are implemented over A^2-MAKE framework.

In the first scenario, it is assumed that CRL is held by mesh clients in addition to the mesh routers. Therefore mesh clients can perform revocation list check by themselves with the CRL obtained from the router it is connected when the updated list is broadcast by the Network Operator to the network through mesh routers. Important problem to be considered here is the possible use of obsolete CRL by the mesh clients acting as relaying agents in revocation list checking.

On the other hand, in the second scenario, CRL is only held by the mesh routers. A relaying mesh client asks the router it is connected, to perform UserRL checking for another client which she assists to connect to the network. As a result, all revocation list checkings are made by the mesh routers with the up-to-date CRL.

In both of these scenarios, it is important to examine the authentication times and the number of successful connections made. In the first scenario, differing from the second one, analysis of the number of true positive authentications made by the relaying mesh clients is required. True positive authentication is the ratio of the number of authentications accomplished by the relaying mesh clients with the up-to-date CRL to the total successful authentications made by her throughout the lifetime of the network including the authentications made with obsolete CRL.

4 Performance of Two Different CRL Distribution Scenarios

In order to evaluate the performance of different CRL distribution schemes, we conducted experiments on ns-3 (version 13) [1], on Ubuntu 10.04 platform.

In all our simulations, the simulated nodes are placed in a 4000m × 4000m square shape area. The number of mesh clients varies between 50 to 300 by 50 increments. Furthermore, the number of routers is taken as 121. The routers are placed at fixed positions on a grid in the network simulation area. The mesh clients start their movements at random points within the area and do random movements within it. The randomness for the users' movements is obtained by the random path generation algorithm provided in ns-3.13. Packet queue size of mesh routers and relaying mesh clients is assumed to be constant, which is set to 10 packets in our simulations, meaning that some of the packets will be dropped if the queue is full. Therefore, increased number of packets causes an increase in the rate of dropped packets.

In our simulations, 30% of the users are assumed to act as routers, i.e. relaying network users (or agents). Relaying users in this network are not assumed to be a part of the network backbone. Unlike the network operator and mesh routers, they have to authenticate with a router first in order to connect to the network and then perform the relaying activity.

All routers are assumed to be informed instantly by the network administrator of the up-to-date CRL using the established network. On the other hand, mesh clients that are acting as relaying agents obtain this updated list from a router only if they are connected to the network. These updates are assumed to be broadcast to corresponding receivers at three different time intervals; 60, 180, and 300 seconds. Furthermore, in every 30 seconds, routers broadcast their public parameters together with a signature, the beacon, to all users in vicinity. In addition, if there are any relaying users connected to the routers, they also broadcast their public parameters along with an anonymous group signature in every 30 seconds. All of the simulations were performed for one-day of simulated time.

Protocol Step	*Party*	*Time (ms) 80-bit (128-bit)*
Verification of an Anonymous Signature	Mesh Router Relaying Agent	401.8 (811.9) 1109 (2.241)
Verification of a Conventional Signature and Anonymous Signature Generation	Mesh Client	229.9 (583.1)
Verification of an Anonymous Signature and Anonymous Signature Generation	Mesh Client	1319 (2774)

Table 1.: Timings for the Protocol Steps performed by the Parties for 80-bit and 128-bit Security

In these simulations, it is assumed that mesh clients, either relaying agent or a normal user, are running the protocol steps on a processor with 800 MHz clock frequency (i.e. timings are taken for the platform with Atom$^{\mathrm{TM}}$ Processor Z500). On the other hand, mesh routers are assumed to be running on a processor similar to the one used in protocol implementations, a dual core 2.26 GHz processor. Timings used in simulations are computed from the results given in Tables 4 and 5 of [4] (cf. Chapter 6) for the 80-bit and 128-bit security levels, respectively.

4.1 Scenario 1: UserRL is held both at mesh routers and mesh clients

In this section, results of the simulations performed considering the three different UserRL broadcast time intervals are analyzed. In this current scenario, where mesh clients hold UserRL locally, time intervals are assumed to be 60, 180, and 300 seconds between each UserRL broadcast.

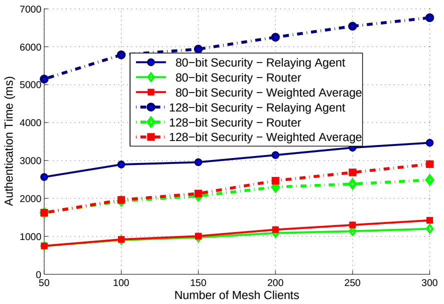

Fig. 2.: Authentication Times for 80-bit and 128-bit Security Levels

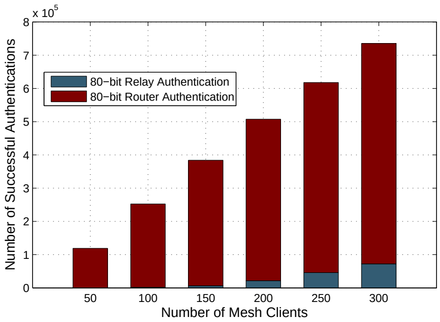

Fig. 3.: Number of Successful Authentications by Routers and Relaying Agents

Figure 2 shows the average authentication time of the mesh clients with respect to the number of the mesh clients within the network for both 80-bit and 128-bit security levels. Average time of the authentications made by mesh routers and relaying mesh clients are shown separately together with a weighted average of them. The average of all timings obtained from three different simulations corresponding to the three different UserRL broadcast time intervals are given as the authentication time. Weighted average is calculated by dividing the total time spent on all successful authentications performed by both parties by the total number of successful authentications.

As seen from Figure 2, ceteris paribus, average authentication time increases linearly with the increasing number of mesh clients. However, average authentication time increases very slowly as the number of mesh clients increases. Weighted average authentication time increases approximately 85%, and 75% at most for 80-bit and 128-bit security levels, respectively, with respect to six-fold increase in number of mesh clients.

Number of successful authentications made by relaying mesh clients and routers for 80-bit security level is given in Figure 3. The results are similar for 128-bit security level. These numbers are used in the calculation of the weighted authentication time and explain why the weighted authentication times in Figure 2 is nearly the same as the average authentication times resulting from the operation performed by the mesh routers. The latter is due to the fact that, on the average, approximately the 95% of all the authentications are accomplished by the mesh routers. Furthermore, the total number of successful authentications made increases linearly with respect to increasing number of mesh clients as expected.

Another important metric is the ratio of successful authentication attempts. This metric is calculated as ratio of the number of successful authentications to the number of authentication requests made. Figure 4 demonstrates the ratio of successful authentication attempts made to the mesh routers and relaying mesh clients separately together with the ratio of the weighted average of these successful authentication attempts for 80-bit and 128-bit security levels. This ratio decreases with the increasing number of mesh clients. This is expected, since the number of packets throughout the network increases with the increasing number of mesh clients, whereas the number of mesh routers stays constant. Furthermore, each mesh router and relaying mesh client can handle only limited number of packets. As it is seen from Figure 4, ratio drops from nearly 0.92

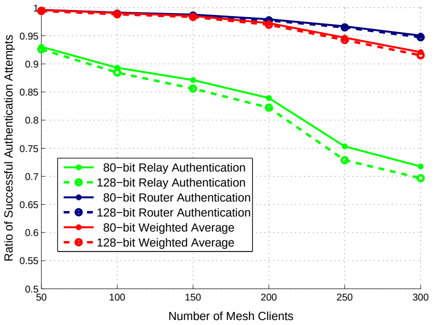

Fig. 4.: Ratio of Successful Authentication Attempts (with Weighted Averages)

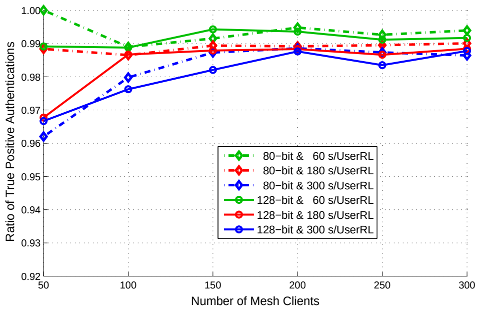

Fig. 5.: True Positive Authentications made by Relaying Mesh Clients

to 0.70 for the authentication attempts made to the relaying agents as number of mesh clients increases from 50 to 300. On the other hand, a decrease in the ratio is also observed for the authentication attempts made to the mesh routers while it is not as steep. Authentication of mesh clients are performed by the mesh routers and relaying agents where all these authenticators perform UserRL checking locally. Although the mesh routers are informed instantly by the network administrator for the updated UserRL, relaying agents are not able to obtain the updated list if they are not connected to the network during UserRL broadcast. As a result, it is possible for a relaying mesh client to perform authentication with an obsolete UserRL. We call the authentications made by relaying mesh clients with the up-to-date UserRL as true positive authentications. In Figure 5, ratio of the true positive authentications made by the relaying agents to the total number of authentications is given. As seen from Figure 5, generally true positive ratio decreases with the increasing UserRL broadcast time interval. However, this behavior becomes less conspicuous with the increasing number of mesh clients within the network. Moreover, security level does not seem to have a meaningful impact on this ratio.

4.2 Scenario 2: UserRL is held only at mesh routers

In this scenario, it is assumed that UserRL is held only at mesh routers and relaying mesh clients do not have access to them. As a result, in order to authenticate another mesh client, relaying agent sends data values used in UserRL checking to the mesh router it is already connected to, and asks this router to perform UserRL checking. In simulations, it is assumed that there are 10 clients in the list throughout the simulated time. Therefore, it is assumed that the mesh routers perform UserRL checking in 0.02026 s, and 0.04909 s for 80-bit and 128-bit security levels, respectively.

Figure 6 shows the authentication time of the mesh clients for 80-bit and 128-bit security levels. Similar to the results obtained from the simulations performed for the

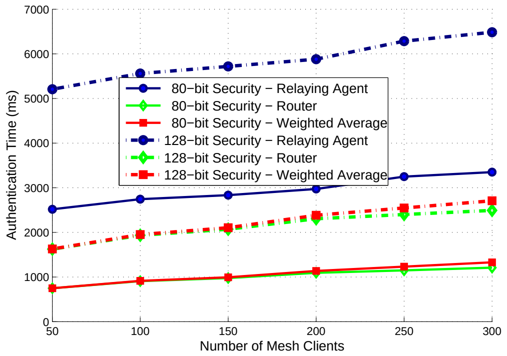

Fig. 6.: Authentication Times for 80-bit and 128-bit Security Levels

first scenario, average authentication time increases linearly with the increasing number of mesh clients. It increases very slowly as the number of mesh clients increases. Weighted average authentication time increases approximately 75%, and 65% at most for 80-bit and 128-bit security levels, respectively, with respect to a six fold increase in the number of mesh clients. Related figure is the number of successful authentications made by relaying mesh clients and router. Figure 7 shows the corresponding results for 80-bit security level. The results are similar for 128-bit security level. The ratio of number of successful authentication attempts to the number of authentication attempts made for the second scenario is given in Figure 8. Figure 8 demonstrates the corresponding ratio for the successful authentication attempts made to the relaying mesh clients and mesh routers separately together with the weighted average of them. Comparing Figure 8 with corresponding Figure 4, it is seen that the ratio of the successful authentication attempts is lower for the second scenario where the UserRL checking is performed only by the mesh routers. This difference is notable in authentications made by the relaying mesh clients. This may be due to the increased packet drops throughout the network and increased response time of the mesh routers to the UserRL checking requests.

As a result, authentication times obtained from the simulations performed for this scenario are mostly lower than the ones obtained in the first scenario. This may occur since the authentications that require more time are possibly dropped, either at the router due to the packet queue being full or within the network, leaving successful attempts having comparatively lower authentication times. This possibly compensates the expected increase in authentication times due to relaying agents waiting acknowledgments for the UserRL checking requests.

Lastly, ratio of true positive authentications is 1.0 in this scenario. This is due to the fact that relaying mesh clients always delegate UserRL checking to mesh routers that possess the up-to-date UserRL.

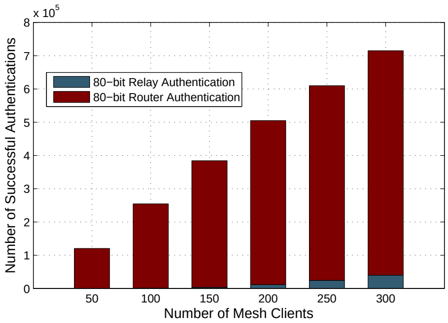

Fig. 7.: Number of Successful Authentications by Routers and Relaying Agents

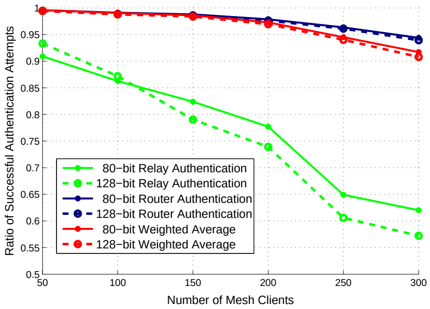

Fig. 8.: Ratio of Successful Authentication Attempts (with Weighted Averages)

5 Conclusion

In this work we conducted simulations on A^2-MAKE anonymous authentication framework in order to address the issue of whether checking CRL in authentication is feasible on relaying agents on time (first scenario) or in a lazy manner by mesh routers only (second scenario) since this may become a serious concern as the number of revoked users increases.

To conclude, although the authentication times for both distribution mechanisms show similar behavior, higher ratio of the successful authentication attempts with respect to the second CRL distribution scenario in addition to the higher levels of true positive authentication favors the first scenario to be accepted as the CRL distribution scheme.

References

1. The ns-3 Network Simulator Available at `http://www.nsnam.org`. Accessed 02-March-2012.
2. Ian F. Akyildiz, Xudong Wang, and Weilin Wang. Wireless mesh networks: a survey. *Computer Networks*, 47(4):445–487, 2005.
3. Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors. *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*, 2004. ACM. ISBN 1-58113-961-6.
4. Ahmet Onur Durahim and Erkay Savaş. A^2-MAKE: An efficient anonymous and accountable mutual authentication and key agreement protocol for WMNs. *Ad Hoc Networks*, 9(7):1202-1220, 2011.