ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Efficient Certificate Validation in Hybrid Mobile Ad Hoc Networks

Mohammad Masdari
Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran,

Sam Jabbehdari
Computer Engineering Department, Islamic Azad University, North Tehran Branch, Tehran, Iran,

Jamshid Bagherzadeh
Department of Computer Science and Engineering, Indian Institute of Technology, Delhi,

Abstract: Providing consistent certificate status information (CSI) in dynamic environment of MANET is a challenging issue. Inconsistent CSI decreases the network security and makes the network vulnerable to CSI replay attacks which previously issued valid CSI are forwarded for the status of a revoked certificate. In this paper, we propose a new certificate validation solution for hybrid MANETs which decreases the OCSP responses' validity period according to the accusations issued against the certificates. As a result, the OCSP responses of revoked certificates will be valid for shorter time and for less time will be available for malicious nodes. Furthermore, in this scheme the number of accusations issued against each certificate is added to the OCSP response's validity period which can be very useful on client side for tuning the certificate validation parameters and localized certificate revocations. Simulation results indicate that our solution effectiveness of our solution.

Keywords: Security, PKI, ADOPT, Verification, Caching node.

I. INTRODUCTION

PKI or Public Key Infrastructure is the combination of software and technologies which enables network users to protect their communications on the Internet [1]. Numerous solutions have been proposed in the literature to adapt PKI for mobile ad hoc networks(MANET) which can be classified as centralized and decentralizedschemes[2].

Certificate revocation is an integral component of certificate management systemswhich tries to isolate attackers from further participating in network activities[3-8].Although some revocation methods[9-14]are proposed for MANETs,the main revocation method is the voting-based revocation mechanismwhich accusations issued by user nodes are collected and weighted according to the accuser's trust level by CA. When the computed value is greater than a specific threshold, CA may decide to revoke the certificate[8, 15-17].

Nevertheless, voting-based revocation suffers from slow attack response because before triggering a revocation order, several attacks are needed to be launched by attacker node. This problem reduces the effectiveness of voting-based revocation and causes the attacker to stay longer in MANET[11].

The other security problems which we face with them in MANET are caused by the inconsistency of certificate validation information. In conventional networks, clientsuse OCSP protocol to get timely information of certificate status [18]. Because OCSP uses small request and response messages,it is more suitable forresource limited MANETs and new emerging computer networks.However, modification is needed to adapt the OCSPprotocolto the dynamic environment of hybrid MANETs[19, 20].

Althoughseveral OCSP-based certificate validation schemes are proposed for MANET,most of them suffer from inconsistency of certificate status information or CSI.

This inconsistent CSI can be misused by attackersto launch various security attacks, because the revoked nodes are still valid for other nodes which have stale and inconsistent CSI. which stale CSI withgood status is forwarded to the client for the status of revoked certificate[21]. This problem creates a window of vulnerability and as a resultthe owner of arevoked certificate isrecognized as a valid node in MANET.

To reduce CSI inconsistency,Papapanagiotou et al. present ADOPT or Ad hoc Distributed OCSP for Trust which by effective use of caching is able to deliver CSI even in the offline states to the ad hoc network nodes[22].

In existing certificate validation schemes, such as ADOPT, the primary technique to reduce theCSI inconsistency is to periodically refresh them in short time periods, but this solution has low scalability and puts heavy loads on the PKI-system and MANET.

As a result, an effective solution is needed to mitigatethe CSI inconsistency with low overheads.In this paper, we propose an ADOPT-based efficient certificate validation solution which we call S-ADOPT or Secure-ADOPT.In this scheme the number of valid accusations is added to the validity period of CSI which will be useful on the client side for tuning certificate validation parameters. By accusation-based management of CSI validity period, our solution tries to mitigate the CSI inconsistency, especially in offline states in which responder nodes are not available. Also our solution effectively alleviates the certificate validation overheads on the OCSP responders and also on the MANET.

The remainder of this paper is organized as following: Section 2 discusses the state of the art certificate status validation schemes designed for MANETs and section 3 presents a brief problem definition.Section 4 illustrates our proposed solutions to optimize the certificate validation in MANET, and, finally,section 5 presentssimulation results and directions for future researches.

II. PROBLEM DEFINITION

In voting-based revocation, accusations issued by user nodes are collected by certificate authority (CA) andthen CAmay decide to revoke the accused certificate.Severalvoting-based revocation solutions have been presented for MANETs[23, 24], for instance in [15], a decentralized certificate revocation scheme presented by Arboit et al., allows the MANET nodes to revoke the certificates of malicious entities by broadcasting accusation messages [25]. Nevertheless, voting-based revocation suffers from the following problems[11]:

a. Vulnerability to selective misbehavior which an attacker reveals the detectable misbehavior to just fewer nodes than the number needed to initiate revocation.
b. Suffering from slow attack response because several attacks are needed to be launched by attacker node before the revocation.

Therefore regarding the voting-based revocation, the question is that, how can we improve thiscertificate management method to better react to attacker nodes?

Also, the other question is that, in large hybrid MANETs which consistent of multiple smaller MANETs how can we inform the accusations which are issued against a certificate owner in one MANET to the other MANETs?

The other problem which we want to deal with it in this paper is the CSI inconsistency.The main reason of this inconsistency is the CSI cachingwhich increases the availability of CSI, especially in the offline states that OCSP responders are not available. The CSI inconsistency problem decreases the network security because the attackers which their certificates are revoked by CA are not recognized by user nodes on time. To overcome this problem, ADOPT protocol tries to periodically achieve new status information from responder nodes. Also, in PS-ADOPT subscribed caching nodes wait to receive new published status information. But, both of these solutions work only in online states which a client or caching node has access to the source of statusinformation. But, the question is that, how can we decrease the CSI inconsistency in offline stateswhich responder nodes are not accessible?Because by misusing the before mentioned inefficiencies,an intelligent attacker can stay longer in MANET.

The next section demonstrates our proposed solution to solve these problems.

III. S-ADOPT

In this scheme we assume that there is a hybrid MANET which applies public-key based cryptography for security purpose andMANET uses a certificate authoritywhich is positioned on the conventional networks.

In OCSP response messages, the *producedAt* and *nextUpdate* fields specify the CSI validity period, but they have not been used effectively in the previous schemes and most of the existing certificate status validation schemes assume the same validity period for all CSI.

As figure 1 exhibitsvoting-based certificate revocation is a death process thatby each accusation, accused certificate approaches one step toward the final revocation.

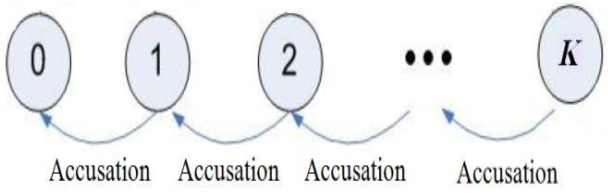

Figure 1: Voting-based revocation

In this paper, we utilize this feature to decrease the validity period of OCSP responses according to the accusations issued against the certificates, and this is performed by setting the value of *nextUpdate* field based on the accusations which are issued against the certificate owner.

As figure 2 indicates, we call the time period between the first accusation and final certificate revocation, as suspicion period.

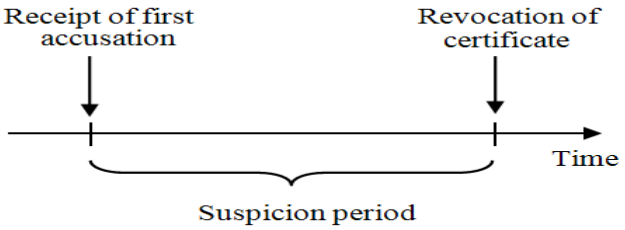

Figure 2: Suspicion period

By decreasing the validity period of OCSP responses in suspicion period, we exhibit that certificate should be less trusted. As a result, the caching period of malicious nodes' CSI decreases and this reduces the inconsistency of OCSP responses in the MANET.Thus as figure 3 indicates by accusation-based decreasing of CSI validity period, our solution achieves lower CSI inconsistency in offline states which responders are not accessible because of link failures, network partitioning and etc.

Furthermore we embed the number of accusations which are issued against the certificate in OCSP responses validity period.

Generally, by effective management of CSI validity period our scheme is aimed to achieve the following advantages:

a. Explicitly transferring the number of accusations which are issued against the certificate owner without any need to alter the OCSP response format and lengthenthe CSI.
b. Decreasing the CSI inconsistency.
c. Reducing the certificate validation overheads on the PKI system.
d. Reducing the reaction time in accusation-based certificate revocations.
e. Better support for the offline validations.
f. Providing more flexible security system which is able to adapt itself to the security situation of MANET environment and achieve more security in more threatened situations with low overhead in more stable times.

However, in this solution to improve the certificate status validation process, we face with some contradicting goals.

For example, in one hand we want to decrease the OCSP responses validity period to mitigate the CSI

inconsistency and on the other hand we want CSI with high validity period to achieve more CSI availability in offline states.

As a result, selecting the right value for validity period of OCSP responses is very important and has direct impact on the factors such as network security, CSI inconsistency and CSI availability.

Interoperability with standard OCSP is one of the important requirements of OCSP-based certificate validation in hybrid networks connected to Internet and other conventional networks. Because our solution does not modify the OCSP request/response messages, it has full interoperability with OCSP protocol. On the other hand, by adding the accusation information to the validity period, not only we try to increase the security of certificate validation, but also we achieve an interoperable scheme with certificate validation standards.

Furthermore, by presenting accusation information to user nodes we provide more support for offline certificate validation and revocation where client nodes must decide about the destination node in the absence of any OCSP responder node.

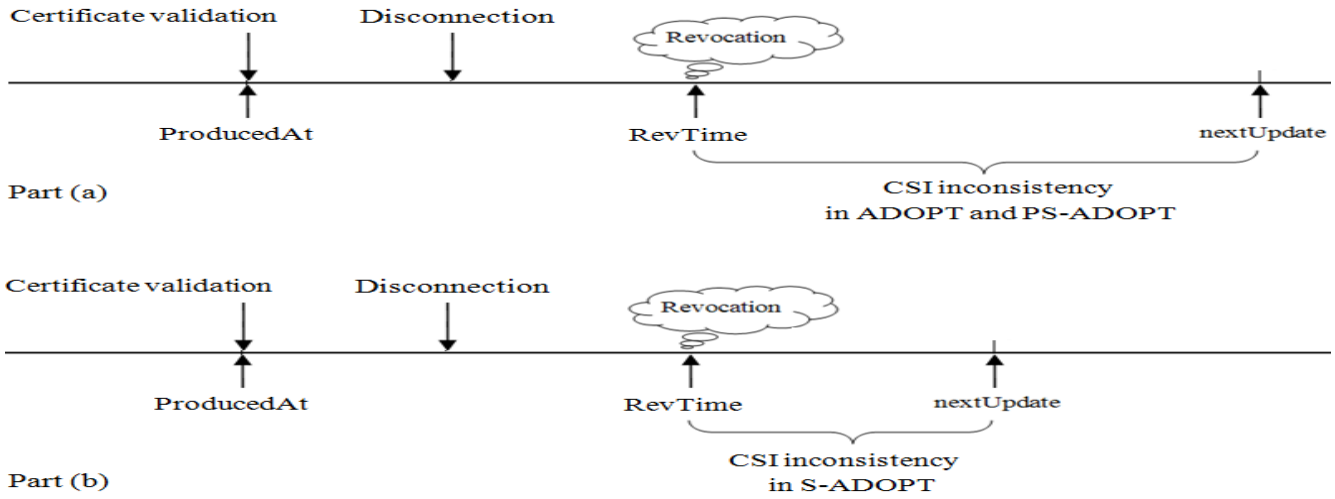

Figure 3: Inconsistency problem in offline states

IV. MANAGING CSI VALIDITY PERIOD

Ideally, we should find a validity periodwhich satisfies the following condition for each newly computed decreased validity period:

$$thisUpdate_i + decValidityPeriod_i = FinalAccussationTime + BlockingPeriod + RevocationDescsionPeriod \quad (2)$$

In this equation $FinalAccussationTime$ is the timeat which a final accusation is issued against the certificate.*BlockingPeriod* is the time period during which the certificate is blocked and PKI-system waits for any vindications, and *RevocationDescsion Period* is the time period which revocation decisions are made by the PKI system. But, we cannot exactly compute the *ith* decreased validity period or $decValidityPeriod_i$ because we do not know the time when the last accusation will be issued.

Generally, the decrease of CSI validity period can be performed by the following methods:

a. Constant decrease.

b. Variable decrease, when different types of accusations are supported.

Constant decrease is the simplest solution which can be used in our scheme. This method needs less information and incurs less overhead on PKI-systems for storing and maintaining information about the different types of accusations for each certificate. Also, by using this method, there is no need for trust management systems to weight the issued accusations. As a result, by using this method only k accusation is needed to revoke the certificate.In this method each accusation decreases the CSI validity period by the following step:

$$DecreasingStep = \frac{BaseValidityPeriod}{K} \quad (3)$$

In this equation, $BaseValidityPeriod$ is the initial validity period for CSI of certificate and *K* is the number of accusations required to revoke it.

Figure 4 exhibits constant decrease in CSI validity periods when some accusations against a certificate occur. According to this figure, the ADOPT and OCSP protocols use the constant validity period and do not consider the node misbehaviors in issuing OCSP responses. As a result, these protocols do not react to changes in the hostility level of destination nodes, and in the absence of any revocation information, user nodes cannot perform certificate validation effectively. But our solution can adapt the CSI validity period according to the behavior of certificate owner and the network security level. However, in the cases when accusations are weighed based on the trust on their issuer, each accusation decreases the validity period according to its weight.In the presence of trust management systems in the network, OCSP responder can apply variable decrease of CSI validity period because accuser nodes may issue different type of accusations and also the trust level of accuser node may differ. In this case, if we assume that *wTotal* is the total required weight to revoke the certificate, then each accusation should decrease the OCSP response validity period by the following decreasing step:

$$DecreasingStep = \frac{w_i}{wTotal} * BaseValidityPeriod \quad (4)$$

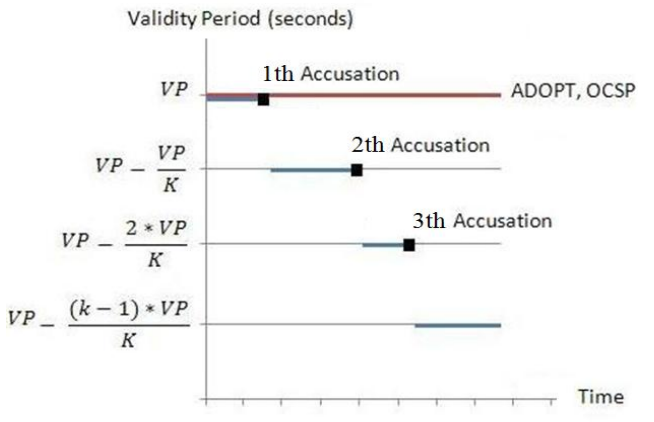

Figure 4: Constant decrease of CSI validity period in S-ADOPT protocol

In this equation, w_i is the weight of *ith* accusation issued against the certificate, and *BaseValidityPeriod*is the initial validity period of OCSP response.

Furthermore,OCSP responder can set the $BaseValidityPeriod$ parameter based on the certificate owner's trust level.

Also, we append the number of accusations issued against the certificate to its CSI validity period.Therefore, using this method, we do not need to alter the OCSP response message formatto add accusation information.

After client receives the requested CSI, it should extract the accusation number from CSI validity period. In this case, when revocation threshold is less than ten, the following equation can be used to extract the number of accusations from CSI validity period:

$$N_{Accusation} = decValidityPeriod_i \ mod \ 10 \quad (5)$$

Nevertheless, when revocation threshold is more than ten, the number of accusations is computed by this equation:

$$N_{Accusation} = decValidityPeriod_i \ mod \ 100 \quad (6)$$

After a user node receivesanew CSI and observesa change in the CSI validity period, itcan take one of the following steps:

a. When CSI's validity period drops to some threshold, user nodes can use the decreased OCSP responses without any refresh rate.
b. If the CSI's validity period is higher than a specific threshold,user nodes can use the OCSP responses with a refresh rate.

Because our solution is an ADOPT-based scheme, when a client node issues a CSI query, it may receive multiple different OCSP responses from the network. As a result, as the following equations indicate, like ADOPT protocol our scheme selects the newest CSI from received results:

$$producedAt_i \geq updateTime_i \quad (7)$$

Where $1 \leq i \leq m$

Accepted CSI=CSI with $Max(producedAt_i)$ (8)

In this equation, $producedAt_i$ is the timeat which*ith*OCSP response is produced, and $updateTime_i$exhibits the end of *ith*CSI validity period.

V. SIMULATION RESULTS

This section demonstrates the experimental setup simulation. For simulation the OMNeT++ simulator [26] is applied which is a discrete event network simulation framework. In this simulator, to evaluate various features of certificate validations we use INET frameworks [27] which contain wireless communicationprotocols. In these simulations we focus on the CSI inconsistency problem. Normally in voting-based certificate revocations, the following factors affect the certificate status inconsistency:

a. Freshness pattern of CSI requests
b. CSI request pattern and arrival rate
c. Suspicion period or the average time period during which all k accusations are issued against the accused certificate
d. Revocation threshold k
e. Certificate status validation protocol

Table 3: Simulation Environment Parameters

General Parameter	**Value**
Terrain dimensions	600m*600m
Number of nodes	20 to 110
Number of OCSP responders	1
Number of caching nodes	10% of network nodes
Cache updating policy	Periodic
Revocation rate	5 or 10 network nodes
Revocation threshold	4, 6 and 8 accusations
CSI queries	Poisson distribution
Mobility	Mass Mobility
Speed	Between 8mps, 20mps
Update Interval	100ms
MAC layer	IEEE 802.11g
Routing protocol	DYMO
Transmitter Power	0.2mW
Parameter for ADOPT	**Value**
ADOPT Request size	66 bytes
ADOPT Response size	187 bytes
Base validity period	200s
Parameters for S-ADOPT	**Value**
Decreasing method	Constant

Although some of these parameters, such as CSI request pattern and arrival rate, cannot be controlled by certificate validation system, other factors such as CSI validity period can be tuned by the PKI system to improve various certificate validation factors. In the rest of this section, we evaluate various factors which affect the inconsistency problem. Table 3 specifies various parameters which have been used in our simulation scenarios.

In this section, we evaluate the simulation results which are conducted in online states which caching node is capable of contacting the responder based on the client demand or certificate validation protocol.

In the first set of experiments, we studied the impact of freshness pattern mainly on CSI inconsistency and also other issues such as cache hit ratio, messaging overheads and processing overheads.

In this scenario,the validity period of CSI is set to 600 seconds, and accusations are issued in the first 600 seconds to revoke the certificates of 5 nodes.Other simulation parameters are specified in table 4.

The first parameter which we measure is the average CSI inconsistency.

Figure 5 shows the comparison of average CSI inconsistency in the S-ADOPT and ADOPT. In this scenario, we issue the CSI requests by 100 and 200 seconds freshness. Also,caching nodes which uses S-ADOPT updatetheir cache in VP/2 and VP/3 time periods and VP is the validity period of received CSI.As this diagram indicates, our solution with constant refreshing presents much lower CSI inconsistency than ADOPT with 100 seconds freshness.

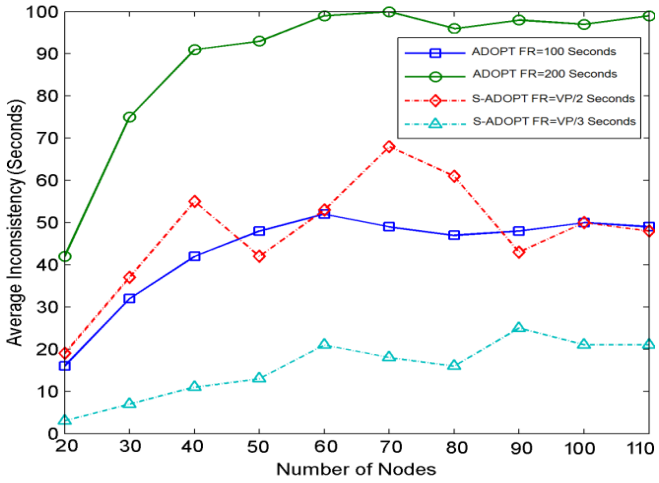

Figure 5: Comparison of average CSI inconsistency, VP=Validity Period, FR=Freshness

However, reducing the CSI inconsistency must not be the final goal, and this should be achieved along with improvements on the other certificate validation parameters such as cache hit ratio as well as processing and messaging overheads.

The next parameter measured in this experiment is the average cache hit ratio in the caching nodes. As indicated in figure 6 our solution efficiently improves the cache hit ratio and presents better results than those of ADOPT with freshness set to 200 seconds.

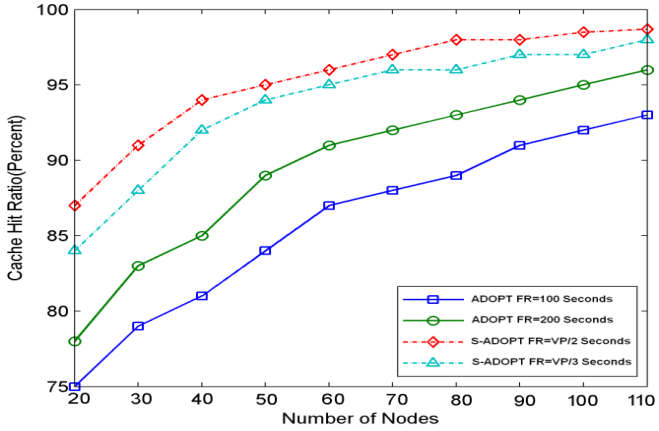

Figure 6: Average cache hit rate in Caching nodes

The diagramin figure 7 indicates the processing loads which S-ADOPT and ADOPT put on the OCSP responder node.This figure supports the results coming from figure 7 and reveals that our solution sends fewer CSI requests to the responder nodes than ADOPT, and it keeps its effectiveness as the number of network nodes increases.

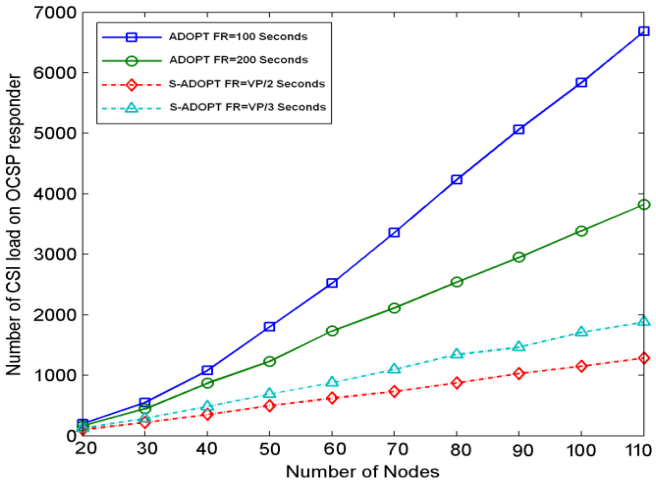

Figure 7: Comparison of processing overheads on OCSP responder, VP=Validity Period, FR=Freshness

The main factor which affects the processing overheads of OCSP responder is the cache miss rate. Regarding the results of figures 7 and 8, we observe that because our scheme has higher average cache hit ratio, it incurs fewer certificate status validation loads on the OCSP responder. Figure 8 plots the number of transmitted bytes for CSI queries which caching nodes send and receive in cache updating operations.

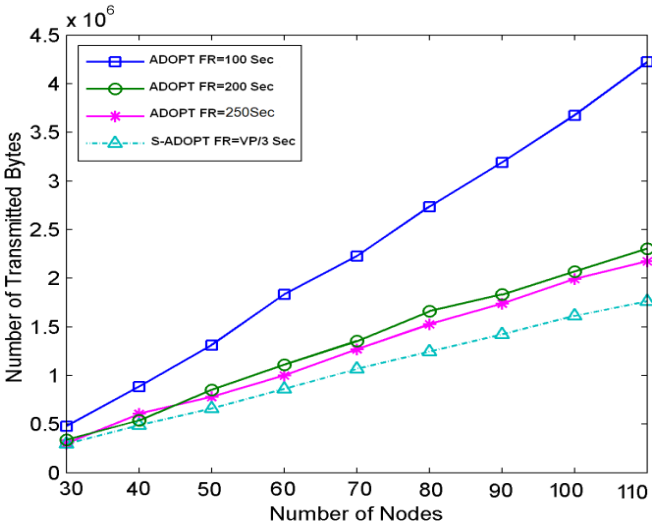

Figure 8: Messaging overheads between Caching nodes and OCSP responder, VP=Validity Period, FR=Freshness

From this figure it can be observed that our protocol effectively decreases the messaging overheads of certificate validation, which is very important in bandwidth limited ad hoc networks. Furthermore, our solution achieves this improvement without modifying request or response messages.

VI. CONCLUSION

In this article, we proposed a new certificate validation solution called S-ADOPT which tries toreduce the CSI inconsistency problem in hybrid MANETs. For this purpose, by each accusation issued against the certificate, validity periods of OCSP response messages are reduced, and also the number of accusations is appended to the validity period. By having accusation-related information, client nodes

which cache the CSI, can better tune OCSP response refresh rate and achieve lower inconsistency with lower overheads.

Thus, our scheme can adapt itself to thesecurity problems of more threatened networks by decreasing the validity period of OCSP responses.

VII. REFERENCES

[1] D. H. Yum and P. J. Lee, "A distributed online certificate status protocol based on GQ signature scheme," in Computational Science and Its Applications–ICCSA 2004, ed: Springer, 2004, pp. 471-480.

[2] M. Omar, Y. Challal, and A. Bouabdallah, "Certification-based trust models in mobile ad hoc networks: A survey and taxonomy," Journal of Network and Computer Applications, vol. 35, pp. 268-286, 2012.

[3] J. Zhang, N. Hu, and M. Raja, "Digital certificate management: Optimal pricing and CRL releasing strategies," Decision Support Systems, 2013.

[4] L. Wei, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Networks," in Communications (ICC), 2011 IEEE International Conference on, 2011, pp. 1-5.

[5] W. Liu, H. Nishiyama, N. Ansari, and N. Kato, "A Study on Certificate Revocation in Mobile Ad Hoc Networks," in Communications (ICC), 2011 IEEE International Conference on, 2011, pp. 1-5.

[6] M. Srividya, K. Radhika, and D. Jamuna, "Review On Certificate Revocation Of Mobile Ad Hoc Networks," International Journal of Engineering, vol. 1, 2012.

[7] S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Securing DSR against wormhole attacks in multirate ad hoc networks," Journal of Network and Computer Applications, vol. 36, pp. 582-592, 2013.

[8] L. H. G. Ferraz, P. B. Velloso, and O. C. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks," Ad Hoc Networks, vol. 19, pp. 142-155, 2014.

[9] I. Bilogrevic, M. H. Manshaei, M. Raya, and J.-P. Hubaux, "Optimal revocations in ephemeral networks: A game-theoretic framework," in Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2010 Proceedings of the 8th International Symposium on, 2010, pp. 21-30.

[10] S. Chinni, J. Thomas, G. Ghinea, and Z. Shen, "Trust model for certificate revocation in ad hoc networks," Ad Hoc Networks, vol. 6, pp. 441-457, 2008.

[11] J. Clulow and T. Moore, "Suicide for the common good: a new strategy for credential revocation in self-organizing systems," ACM SIGOPS Operating Systems Review, vol. 40, pp. 18-21, 2006.

[12] M. F. Hinarejos, J. L. Muñoz, J. Forné, and O. Esparza, "PREON: An efficient cascade revocation mechanism for delegation paths," Computers & Security, vol. 29, pp. 697-711, 2010.

[13] T. Panke and B. Pati, "Improved Certificate Revocation Method in Mobile Ad Hoc Network," International Journal of Computer Applications, vol. 80, 2013.

[14] I. Bilogrevic, M. H. Manshaei, M. Raya, and J.-P. Hubaux, "OREN: Optimal revocations in ephemeral networks," Computer Networks, vol. 55, pp. 1168-1180, 2011.

[15] G. Arboit, C. Crépeau, C. R. Davis, and M. Maheswaran, "A localized certificate revocation scheme for mobile ad hoc networks," Ad Hoc Networks, vol. 6, pp. 17-31, 2008.

[16] K. Prasanth and P. AnbuKumar, "SECURE CLUSTER FORMATION AND CERTIFICATES REVOCATION FOR ADVERSARY NODES IN THE MOBILE AD HOC NETWORK."

[17] H. Dahshan, F. Elsayed, A. Rohiem, A. Elgmoghazy, and J. Irvine, "A Trust Based Threshold Revocation Scheme for MANETs," in Vehicular Technology Conference (VTC Fall), 2013 IEEE 78th, 2013, pp. 1-5.

[18] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 Internet public key infrastructure online certificate status protocol-OCSP," RFC 25601999.

[19] Y. Dong, A.-F. Sui, S.-M. Yiu, V. O. Li, and L. C. Hui, "Providing distributed certificate authority service in cluster-based mobile ad hoc networks," Computer Communications, vol. 30, pp. 2442-2452, 2007.

[20] P. Khatri, "Using identity and trust with key management for achieving security in Ad hoc Networks," in Advance Computing Conference (IACC), 2014 IEEE International, 2014, pp. 271-275.

[21] G. F. Marias, K. Papapanagiotou, V. Tsetsos, O. Sekkas, and P. Georgiadis, "Integrating a trust framework with a distributed certificate validation scheme for manets," EURASIP Journal on Wireless Communications and Networking, vol. 2006, pp. 77-77, 2006.

[22] K. Papapanagiotou, G. F. Marias, and P. Georgiadis, "Revising centralized certificate validation standards for mobile and wireless communications," Computer Standards & Interfaces, vol. 32, pp. 281-287, 2010.

[23] M. T. Panke, "Clustering Based Certificate Revocation Scheme for Malicious node in MANET," International Journal of Scientific and Research Publications, vol. 3, 2013.

[24] E. Neena and C. Balakrishnan, "Cluster Based Certificate Revocation of Attacker's Nodes in MANET," 2014.

[25] K. Park, H. Nishiyama, N. Ansari, and N. Kato, "Certificate revocation to cope with false accusations in mobile ad hoc networks," in Vehicular Technology Conference (VTC 2010-Spring), 2010 IEEE 71st, 2010, pp. 1-5.

[26] "OMNeT++ Simulator," p. http://www.omnetpp.org.

[27] "INET frameworks " p. http://inet.omnetpp.org/