A Certificate Revocation Scheme for Wireless Ad Hoc Networks

Claude Crépeau* and Carlton R. Davis*
School of Computer Science, McGill University,
Montréal, QC, Canada H3A 2A7.
[crepeau, carlton]@cs.mcgill.ca

ABSTRACT

The increasing prominence of wireless ad hoc networks is stimulating greater interest in developing adequate security mechanisms for securing applications involving these innovative networks paradigms. To-date, the proposed security schemes either provide inadequate security or they are too costly computationally, and therefore impractical for most ad hoc network applications.

Adapting wired network security schemes—particularly those involved digital certificates—to wireless ad hoc networks environments, poses many difficulties, primarily for two reasons: the limitation of computational resources, and the absence of centralized entities for performing critical key management tasks such as certificate revocation.

In this paper, we propose a certificate revocation scheme for wireless ad hoc networks. Our revocation scheme not only provides a measure of protection against malicious accusation attacks, but it also effectively eliminates the window of opportunity whereby revoked certificates can be used to access network services.

Keywords

Revocation scheme, ad hoc network security, public-key cryptography, digital signature

1. INTRODUCTION

As is the case with practically all existing network architectures, rather than being an integral part of the architectural design of ad hoc networks, security related issues have been more so treated as after-thoughts. Routing, pertinent physical-layer and data-link layer issues such as medium access and error correction, respectively, have received much attention in early research efforts [6, 8, 11, 12, 18, 21, 26, 29]. On the contrary, security issues attracted rather limited attention. As the prominence of ad hoc networks increase, however, security related issues are gradually brought to the forefront.

*Supported by NSERC and Alcatel Canada.

Proceedings of the f[t] ACM Workshop Security of Ad Hoc and Sensor Networks Fairfax, Virginia

Security requirements of wireless ad hoc networks are similar to that of other networks. They can be briefly summarized as follows:

- *Access control:* The need to restrict access of network resources to legitimate authorized entities.
- *Authentication:* Guarantee of the authenticity of the network peers and traffic source; that is, provides some assurance that a given network node is actually who it claims to be, and that any given network traffic actually ordinated from the source it proports to originate from.
- *Confidentiality:* Provides assurance that data in its un-obfuscated form will be restricted to legitimate entities that have the authority to access the data.
- *Availability:* Network resources should be available to authorized entities without excessive delays.

Different networks have different security requirements. For example, a military network, or any networks involved in the transmission of sensitive information, will likely have greater need for confidentiality services than a network consisting of, for example, household appliances. Perhaps, the security service that is a basic requirement of most networks is access control. Unlike wired networks which can employ physical security mechanisms such as perimeter boundaries that help to restrict access to a network infrastructure, ad hoc networks—by virtue of the fact that the transmission medium is wireless—are far less restrictive. The need for access control is therefore more apparent.

Interestingly, the phenomena that make ad hoc networks paradigms so attractive: being self-organizing, dynamic and decentralized, are the same phenomena that compound the challenges of developing adequate security mechanisms for these networks. Consider for example the difficulty associated with the use of digital certificates in ad hoc networks. If the nodes have the necessary computational resources for handling public-key cryptography, then the remaining challenges can be briefly outlined as follows:

1. *Issuing of certificates*
2. *Validating certificates*
3. *Storage and retrieval of certificates*
4. *Revocation of certificates*

The first three items can be dealt with in an intuitive way. Yes, there are no centralized entity in ad hoc networks to play the role of certificate authorities (CAs). However, as is the case with wired networks with high security requirements, whereby entities identities are verified off-line before certificates are issued; the same principle can be applied for ad hoc networks. Network nodes can be required to have valid certificates from trusted CAs prior to joining the network. The validation of certificates can be easily done if each node stores the public keys of the trusted CAs that issued the certificates of the peers it needs to communicate with. Similarly, each node can store the certificates of its communicating peers; thus the certificates will be readily available when they are required.

The greater challenge is certificate revocation. For various reasons, certificates will need to be revoked periodically; for example, if the private key associated with a certificate is compromised, the certificate will need to be revoked and information be made available to network peers in a timely manner. For conventional networks, CAs issue certificate revocation lists (CRLs)—containing information about revoked certificates—at regular intervals. The CRLs [16] are either placed in online repositories where they are readily available, or they may be broadcast to the individual nodes. Alternatively, online certificate status protocol (OCSP) [23], can be used to ascertain information about the status of a certificate. The interested reader can refer to [23] or [7] for further detail on OCSP.

Whether CRLs, OCSP, or any other certificate validation protocols, are used in the traditional networking settings, a necessary requirement is the availability of network connection to the CAs, the central repositories where CRLs are stored, or to the centralized servers running the certificate validation protocols. The problem with adapting this scenario to ad hoc network is: in any given ad hoc network, there may neither be network connection to centralized CAs nor central repositories where CRLs can be retrieved, or centralized servers running certificate validation protocol(s). Thus, ascertaining whether or not a certificate is revoked presents a challenge in ad hoc networks environments.

To-date, the security schemes utilizing digital certificates, proposed for ad hoc networks, either do not explicitly address the issue of certificate revocation, or they require that certificates of nodes be revoked when the nodes are accused of misbehavior. Either approach can be problematic. Certificate revocation is too important an issue to be ignored; nonetheless, if adequate safeguards are not built into the process of determining when a certificate should be revoked, malicious nodes can wrongfully accuse other nodes of misbehavior and cause the certificates of good, uncompromised nodes to be revoked. Compromised or malicious nodes can in fact use this phenomenon (we called it malicious accusation) as an exploit for isolating and ultimately cutting off legitimate, well-behaving nodes from a network.

In this paper we proposed a certificate revocation protocol for ad hoc networks, that provides a measure of protection against malicious accusation attacks. The protocol allows individual nodes to use commonly agreed upon criteria to revoke certificates. Information that are used to decide whether or not a certificate should be revoked, is shared by all the nodes; however, it is the individual nodes that are given the responsibility of revoking certificates and storing information about the status of the certificates of the peers they communicate with. Certificate status information is thus readily available to each node; consequently, enabling the elimination of the window of opportunity whereby revoked certificates can be accepted as valid.

The rest of the paper is organized as follows: Section 2 reviews some of the proposed security solutions for addressing access control, authentication and confidentiality services in ad hoc networks, and highlights their merits and drawbacks. Section 3 presents the details of our proposed revocation scheme, and its merits are discussed in Section 4. Finally, Section 5 summarizes our contributions in this paper.

2. MOTIVATION

The security solutions proposed for addressing access control, authentication or confidentiality service requirement of ad hoc networks, utilized the following technologies:

1. *Symmetric-key cryptography*
2. *Digital certificates*
3. *Threshold cryptography*

In this section, we highlight advantages or drawbacks of using these technologies to address the security need of ad hoc networks; and review some of the proposed security solution published in open literature. We commenced with symmetric-key cryptography.

2.1 Symmetric-key based solutions

Security solutions based on shared symmetric keys have their virtues: asymmetric cryptographic schemes are much more computationally intensive than symmetric-key schemes of comparable strength. Network security applications that are based solely or predominantly on symmetric-key cryptography, in general, have considerably lower overhead, and consequently afford lower reduction in throughput than applications based solely or predominantly on asymmetric-key cryptography.

Shared symmetric-key schemes however—whether they are used to provide authentication, access control or confidentiality services—have some noticeable shortcomings, as outlined below:

- *Greater probability of shared key being compromised*: If a secret key is shared among a network of N nodes, the probability of the key being discovered, increases

proportionally with N. Therefore, for optimum security, it is necessary for the key to be changed at high frequency.

- *If a single node is compromised, the entire network can be compromised*: The discovery of the secret key on a single node, means that this key will need to be discarded and a new key distributed to all the nodes that shared it. If there are no key exchange mechanisms in place, the keys would need to be distributed through secure out-of-band means. This could be rather time consuming and problematic for medium or large-scaled networks.
- *Scalability issues*: As outlined above, if a secret key is shared amongst a group of nodes, it is necessary that the key be changed periodically; the frequency depends on the level of security desired. Since the new keys need to be distributed by secure out-of-band means, this might not be an issue for small networks; however, for larger networks, this task could be quite tedious and problematic, and is therefore not a scalable solution.

Wired Equivalent Privacy (WEP) protocol: the security mechanism used by IEEE 802.11 WLAN [13] is an example of a security scheme based predominantly on symmetric-key cryptography. Additional problems associated with WEP are documented in [3, 2, 1].

2.2 Solutions utilizing digital certificates

Digital certificates are important elements in most commonly used network security applications, particularly those providing authentication services. Perhaps the single feature that accounts for the attractiveness of digital certificate technology, is the key management issues it favorably addresses, as summarized below:

- *Simplify key distribution*: Digital certificates do not need to be kept private. There is therefore no need for secure channels for mere key distribution. It suffices to store the certificates in repositories where they can be publicly accessed.
- *Reduced effect of compromise*: If the private key associated with a given certificate is compromised—unlike the case of shared secret-key technology, which necessitates the issuing of a new key to all the entities sharing the key—in most cases, it suffices to replace only the certificates whose associated private keys have been compromised.

However, as outlined in Section 1, there are problems associated with using digital certificate technology in ad hoc networks environments. Digital certificates, generally were designed to be used in centralized environments. Customerly, centralized CAs are required to issue and revoke certificates. Certificates and CRLs are usually stored in centralized repositories. The challenge for ad hoc networks is that there are no centralized entities in these networks. The public keys of the relevant CAs can be stored on the peers and thus be used to verify the validity of the certificates issued by the respective CAs. However, since the peers in an ad hoc network may not have network access to any online entities to ascertain whether or not a certificate has been revoked—in the absence of an effective key management scheme providing up-todate, reliable certificate revocation information—there is a window of opportunity whereby revoked certificates may be accepted as valid.

To-date, none of the proposals published in open literature addresses these concerns. Venkatraman and Agrawal [30] proposed an authentication scheme utilizing digital certificates; quite notably, the proposal does not address the issue of key revocation. In any application involving the use of digital certificates, certificates will need to be revoked periodically. The issue of certificate revocation is therefore too important to ignore.

Candolin and Kari [4] proposed a network architecture for wireless ad hoc networks which utilizes digital certificates to establish trust. The authors outlined that a node within a network may declare another node as being compromised; this ultimately may result in the revocation of trust for the accused node(s). The question that surfaces here that the proposal does not address is, what prevents nodes from wrongfully or maliciously accusing other nodes of misbehavior? The phenomenon of malicious accusation is a tool that malicious agents can use against un-cooperating nodes in attempt to wrongfully cut off network access to legitimate, trustworthy nodes. Provisions therefore need to be made to prevent malicious accusation succeeding in isolating trustworthy nodes.

Hubaux *et al* in [17] proposed a public-key distribution system similar to PGP [32] web of trust model, in the sense that the certificates are issued and revoked by the users. This scheme, addresses the decentralized nature of certificate management in ad hoc networks. However, as is the case with the web of trust model, Hubaux *et al* scheme is susceptible to a high probability of likely infiltration by malicious agents; since all it takes is a single user to issue a certificate to a malicious agent which in turn can issue certificates to several other malicious agents.

2.3 Solution based on threshold cryptography

The idea of (k, n) threshold scheme was introduced by Shamir in [27]. A (k, n) threshold scheme allows a secret, for example a CA signing key, to be split into n shares such that for a certain threshold $k < n$, any k components could combine and recover the signing key; whereas $k - 1$ or fewer shares are unable to do so. Shamir's scheme is based on polynomial interpolation. Variants include: verifiable secret sharing (VSS) [5, 9, 10, 24, 25] and proactive secret sharing [15]. The former allows recipients of shares to verify whether or not the shares are consistent; while the latter provides protection against persistent mobile adversaries, by renewing the shares periodically. Robust threshold signature schemes have been developed for both RSA and discrete log based digital signature algorithms [28, 14].

The idea of utilizing threshold cryptography to distribute trust in ad hoc networks was proposed by Zhou and Haas in [31]. The authors articulated that the challenges associated with key management services (issuing, revoking and

storing of certificates) in ad hoc networks can be resolved by distributing CA duties amongst the network nodes. For example, a CA signing key can be partitioned into n shares and distributed to n nodes. Any k of the n nodes could then collobrate to sign and issue valid digital certificates; whereas a coalition of $k-1$ or less nodes would not be able to do so. Kong *et al* [20, 19] and Luo *et al* [22] proposed and implemented variant solutions based on this idea.

2.3.1 Difficulties associated with implementation of threshold cryptography schemes

Threshold cryptographic solutions may not be suitable for most commercial ad hoc networks environments, for the following reasons:

1. *Computationally exhaustive*: Threshold cryptography involves additional computationally intensive modular exponentiations compared to the underlined asymmetric-key cryptographic protocols. Most low-powered wireless nodes do not have the resources to handle such computationally intensive operations. For nodes with less resources constraints, the increase in latency due to the extra computational cost, may not be acceptable. For example, the analysis of the implementation in [22] indicates that generation of a partial RSA signature using one of k shares, is approximately 2.5 times slower than standard RSA signing. Considering that k partial signatures need to be generated then combined to obtain a valid signature, the increase in latency due to the additional computations may not be acceptable.

2. *Requires unselfish cooperation*: Network security solutions involving threshold cryptography require unselfish cooperation of the communicating peers. This might not be an issue in certain military applications; however, in most commercial network applications nodes may not behave unselfishly. Wireless nodes are often limited in battery power and utilize power conservation mechanisms that encourage them to remain dormant unless they are performing necessary services. It might not be realistic therefore to expect nodes in certain environments to behave unselfishly and cooperate, for example to service certificate requests.

2.4 Summary

In this section, we articulated that network security schemes based solely on symmetric-key cryptography are limited in the security they provide, owing to the increased probability of the shared key being compromised. These schemes, also do not afford scalable solutions in light of the problematic nature of key management issues, such as key renewal.

Ad hoc network security schemes utilizing threshold cryptography, potentially provide greater flexibility and security. However, the computational cost, particularly for low-powered wireless nodes, might be too prohibitive. In addition, these schemes require unselfish cooperation of the communicating peers, which cannot be guaranteed in certain networks environments.

For networks with nodes capable of handling asymmetric-key cryptography, security schemes utilizing conventional digital certificates, offer the best combination of security verses throughput and flexibility. However, there are many challenges associated with using digital certificate technology in ad hoc networks environments, owing to the decentralized nature of these networks. Chiefly among these challenges is the need for efficient key management schemes that effectively address issues such as certificate revocation. In the following section, we outline a proposed certificate revocation scheme for ad hoc networks, that provide some measure of protection against malicious accusation succeeding in causing the revocation of certificates of trustworthy, well-behaving nodes. Our scheme also effectively eliminates the window of opportunity whereby a revoked certificate can be accepted as valid.

3. PROTOCOL DETAIL

In our scheme, the individual nodes within a network are responsible for all key management tasks, except issuing of certificates. Prior to entering a network, a node is required to have a valid certificate issued by a CA that is trusted by the other network peers. It is also expected to have the public keys of the CAs that issued the certificates of the peers it expects to communicate with.

The first duty of a node after entering a network is to broadcast its certificate to all the nodes, and simultaneously sends a request that the nodes send their profile tables. The profile table contains information about the behavior profile of each node in a network. The information in the profile tables is used to determine whether or not a given certificate should be revoked. Each node is required to compile and maintain a profile table. A profile table can be represented in the form of a packet of varied length depending on the number of accusation launched against the nodes. The length ranges from a minimum of 80 bits—when there are no accusation—to a maximum of $97(N-1)+147$ bits, where N is the number of nodes in the network. Details of the fields and content of the profile table are as follows:

1. *Owner's ID*: This field is the first 32 bits of the profile table. It contains an integer indicating the serial number of the owner's (the node that compiled the profile table) digital certificate.

2. *Node count*: this is a 16-bit field containing a short integer indicating the owner's perspective regarding the current number of nodes (N) in the network. We explain how the value of N is ascertained in the section that follows.

3. *Peer i ID*: This is a 32-bit field containing the certificate serial number of a node that is accused of misbehavior. This field also serves the purpose of a marker: if it contains zero, it indicates the end of the profile table.

4. *Certificate status*: This field contains a 1-bit flag; it is set if the certificate of peer i is revoked and unset otherwise.

5. *Accusation info*: This is a 64-bit field; the first 32 bits contains an integer indicating the certificate serial number of a node that accused peer i of misbehavior. The remaining 32 bits contains the date that the accusation was made.

If field 3 does not contain zero, the profile table continues with the certificate status and accusation info fields; and if there are more than one accusers, it continues with 97-bit blocks containing information about other accusers. Figure 1 illustrates the fields of a profile table.

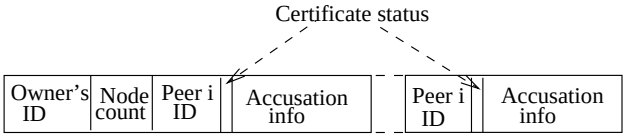

Figure 1: Fields of a profile table

The information regarding the number of accusations, the identity of the accusers, the nodes being accused and the date the accusation was made, should be consistent in all the profile tables. If the node requesting the profile tables, notices any inconsistency, it is expected to launch an accusation against the node(s) that sent the inconsistent data. Profile table data is assumed to be inconsistent if it differs from the data contained in the majority of the other profile tables. Finally, the node compiles its own profile table based on the data the majority of the profile tables contain.

It should be noted that a node is allowed to accuse a given node only once throughout the lifetime of a certificate. Therefore, when an accusation is broadcast, the nodes are required to check the data in their profile tables, and add the information regarding the new accusation (certificate serial number of the accuser and the node being accused, and the date), only if there is no prior record of the accuser accusing that particular node.

Determining the node count

Ad hoc networks are dynamic in nature: network membership and consequently the node count of a given ad hoc network, on average, changes more frequently than other networks of similar size. Our certificate revocation protocol uses the node count (N) as a parameter in certain calculations; therefore, provision needs to be made for a node to determine the number of nodes in the network at any given time.

As outlined earlier, the first duty of a node on entering a network is to broadcast its certificate to its peers. Upon receiving the broadcast, the peers are expected to send their certificates to the new node. The certificates can be stored using any appropriate data structure. However, our protocol stipulates that each certificate entry should contain a field for storing an associated date. The date—including the time—that the certificate was received should initially be stored in this field.

After broadcasting its certificate, each node is required to broadcast short messages—containing its certificate serial number and the date and time that the message was sent—at a configurable time interval of T minutes. The value of T depends on the frequency of the change in the network membership. We called these messages, membership confirmation messages. When a node receives a membership confirmation message, it updates the date field associated with the certificate entry for the sender of the message, with the date indicated in the message.

If a node does not receive a membership confirmation message from any given node within $2T + 1$ minutes, the certificate entry for the node in question, should be deleted from the node's certificate repository. The number of entries in the certificate repository for any given node, should therefore closely reflects the actual number of nodes in the network.

3.1 Stipulation for certificate revocation

In addition to a profile table and a certificate repository, each node is required to compile and maintain a status table. Initially, it is compiled from the data in the profile table, and updated simultaneously along with the latter when a new, pertinent accusation is received. The status table is used to ascertain the status of a certificate; it consists of the following info:

- *Number of accusations against node i (A_i)*: The total number of accusations—limited to one per node—made against node i.
- *Number of additional accusations made by node i (α_i)*: The total number of accusations—limited to one per node—made by node i, minus one.
- *Behavior index of node i (β_i)*: The behavior index of a node i (β_i) is a number such that $0 < \beta_i \leq 1$. It is a measure of the status of a node amongst its peers. The greater the value of β_i, the higher the status of the given node i. β_i is computed as follows:

  $$\beta_i = 1 - \lambda A_i \quad (1)$$

  $\lambda = \frac{1}{2N-3}$, where N is the node count.
- *Weight of node i accusation (ω_i)*: The weight of a node accusation or potential accusation (if the node has not made any accusation to-date), depends on the node's behavior index and the number of accusations it made. ω_i is a number such that $0 \leq \omega_i \leq 1$. It can be calculated as follows:

  $$\omega_i = \beta_i - \lambda\alpha_i \quad (2)$$

  Similarly, $\lambda = \frac{1}{2N-3}$, where N is the node count.
- *Revocation quotient (R_j)*: This number determines whether or not the certificate for node j should be revoked. It is computed as follows:

  $$R_j = \sum_{i=1}^{N} \sigma_{ij}\omega_i \quad (3)$$

  If an accusation graph is constructed using the data in the profile table, such that the nodes of the graph represent the network nodes, and the edges represent accusations; then $\sigma_{ij} = 1$ if there is a directed edge E_{ij} from node i to node j, or 0 otherwise.
- *Certificate status (C_i)*: Indicates whether or not the certificate of node i is revoked.

The revocation quotient threshold (R_T) is a configurable parameter: its value depends on the sensitivity of the security requirement. Typically R_T could be equal to $\frac{N}{2}$, where N is the number of nodes in the network. If $R_j \geq R_T$, then the certificate of node j is revoked and indicated in the certificate status field of the status table. Since the nodes are required to update their profile and status tables immediately after a new, pertinent accusation information is received, the data in the status table should be similar for all the nodes. Therefore, when the R_j value of a node j exceeds R_T, the certificate for this node should be indicated as revoked, simultaneously in the status tables of all the network nodes. Hence, the window of opportunity whereby a revoked certificate can be accepted by a node as valid is practically non-existent.

Nodes whose certificates are revoked are denied network access.

4. DISCUSSION

As mentioned previously, in our scheme, the nodes are responsible for all key management tasks except issuing of certificates. It should not be necessary for the nodes to be involved in issuing of certificates. As is the case with wired networks, where stringent security is required, The CAs should verify the identity of the respective nodes offline before certificates are issued. Therefore, nodes should be required to have valid certificates prior to entering a network.

When a node enters a network, it broadcasts its certificate along with a request that it be sent the profile table of all the nodes. Upon receiving the certificate, each node verifies its validity and stores it if it is valid and it is not in its certificate repository; then it sends its certificate along with its profile table. If the certificate is revoked or if it is invalid, it is discarded and the request for its profile table ignored.

Why requesting profile table? Ad hoc networks are dynamic and their topologies can change frequently. It is important for all the nodes to have consistent data. Therefore, it is necessary that newly arrived nodes be sent the profile data of all the current network nodes. It should also be noted that information about revoked certificates are not deleted from the profile table; they are kept there so that newly arrived nodes can be informed about the revoked certificates, and the identity of the accusers that lead to the revocations.

Why a status table in addition to a profile table? Since the profile table needs to be broadcast to newly arrived nodes, it is important that its size be kept to a minium in order to reduce bandwidth utilization. There is no need to broadcast information about β_i, ω_i and R_j, since they can be calculated locally. Hence, these parameters are stored in a separate table.

4.1 Underlined principle of scheme

The principal aim of the scheme we presented is to prevent malicious accusations from succeeding in causing the revocation of certificates of well-behaving, trustworthy nodes. Secondly, to eliminate or considerably reduce the window of opportunity whereby revoked certificates can be accepted as valid. Our scheme is based on the premise that all accusations should not be treated equally.

If a number of accusations are made against a given node, it is likely that the node is indeed malicious or misbehaving; and therefore, accusations from this node should have less weight than those from nodes with no accusation against them. Similarly, if node i launched multiple accusations against other nodes—particularly if accusations are not supported by more than one of the other nodes—there is an increased probability that this node in question (node i) may be malicious; and therefore its accusations should be given less weight than those from nodes that made smaller number of accusations.

We used the term *behavior index (β_i)* to indicate the assumed status of a node. From equation (1), with $\lambda = \frac{1}{2N-3}$, where N is the node count; it is trivial to show that $0 < \beta_i \leq 1$. A node i with $\beta_i = 1$ is assumed to be a well-behaving, unsuspicious node. The smaller the β_i value the more suspicious a node is assumed to be, and consequently, the smaller the weight of its accusations.

The weight of an accusation from a node i (ω_i), is assumed to be directly related to β_i and inversely related to the number of accusations node i made. From equation (2), again with $\lambda = \frac{1}{2N-3}$, it is also trivial to show that $0 \leq \omega_i \leq 1$.

Weighted accusation has the effect of requiring additional accusation(s) to revoke a certificate when one or more of the nodes accusing the node in consideration, is/are suspicious. As an illustration, consider the following example illustrated using the accusation graph shown in Figure 2. The status

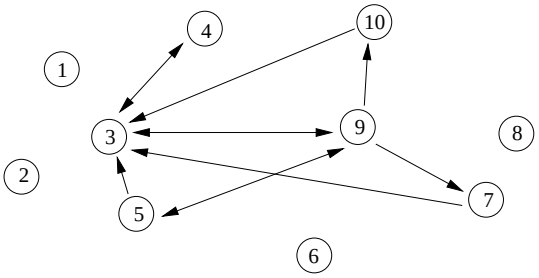

Figure 2: Illustrated accusation graph

table for this accusation graph is illustrated in Table 1.

With the accusation quotient threshold (R_T) set at $\frac{N}{2} = 5.00$, note that even though the number of accusations against node 3 is equal to R_T; however, because an accuser, in this example node 9, is suspicious—owing to the number of nodes it accused—the revocation quotient:
$R_3 = 0.88 + 0.88 + 0.88 + 0.65 + 0.88 = 4.17$ is less than the threshold required to revoke a certificate. Therefore, if node 3's certificate is to be revoked, at least one additional accusation from another node with $\omega_i \geq 0.83$ is required.

Our scheme, thus provides an extra layer of caution in preventing the revocation of certificates owing to malicious accusations. Also, as previously asserted, the fact that the

Table 1: Status table for accusation graph of Figure 2

Nodes	A_i	β_i	α_i	ω_i
1	0	1.00	0	1.00
2	0	1.00	0	1.00
3	5	0.71	2	0.59
4	1	0.94	1	0.88
5	1	0.94	1	0.88
6	0	1.00	0	1.00
7	1	0.94	1	0.88
8	0	1.00	0	1.00
9	2	0.88	4	0.65
10	1	0.94	1	0.88

nodes have identical accusation data in their profile table, and are expected to update their profile and status tables immediately after new, pertinent accusation data is received, if a certificate has $R_j \geq R_T$, it is revoked promptly and simultaneously on all the nodes. Therefore, the window of opportunity whereby a revoked certificate can be accepted as valid, is effectively eliminated.

5. CONCLUSION

In this paper, we assert that network security schemes based solely on symmetric-key cryptography are limited in the security they provide, owing to the increase probability of the shared key being compromised. These schemes, also do not afford scalable solutions in light of the problematic nature of key management issues, such as key renewal.

Ad hoc network security schemes utilizing threshold cryptography, potentially provide greater flexibility and security. However, the computational cost, particularly for low-powered wireless nodes, might be too prohibitive. In addition, these schemes require unselfish cooperation of the communicating peers, which cannot be guaranteed in certain networks environments.

For networks with nodes capable of handling asymmetric-key cryptography, security schemes utilizing conventional digital certificates, offer the best combination of security verses throughput and flexibility. However, there are many challenges associated with using digital certificate technology in ad hoc networks environments, owing to the decentralized nature of these networks. Chiefly among these challenges are the need for efficient key management schemes that effectively address issues such as certificate revocation. In this paper, we proposed a certificate revocation scheme for ad hoc networks, that addresses some of these challenges.

Future work

Our future work includes doing further explorations to evaluate our protocol through security analyses and simulations to access its robustness and its cost in terms of overhead and throughput. We intend to present the results of the further investigations in another publication.

Acknowledgments

The authors are thankful to Yasmin Adu-Arthur for her help in proof-reading. We also would like to thank the anonymous reviewers for their suggestions.

6. REFERENCES

[1] W. A. Arbaugh. An inductive chosen plaintext attack against wep/wep2. IEEE Document 803.11-01/230, May 2001.

[2] W. A. Arbaugh, N. Shankar, and Y. J. Wan. Your 802.11 wireless network has no clothes. In *Proceedings of IEEE International Conference on Wireless LANs and Home Networks*, December 2001.

[3] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. In *Proceedings of ACM International Conference on Mobile Computing and Networking*, pages 180–189, July 2001.

[4] C. Candolin and H. Kari. A security architecture for wireless ad hoc networks. In *Proceedings of IEEE Milcom 2002*, October 2002.

[5] B. Chor, S. Goldwasse, S. Micali, and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Proceedings of 26th IEEE Annual Symposium on the Foundations of Computer Science (FOCS)*, pages 383–395, October 1985.

[6] B. H. Davies and T. R. Davies. The application of packet switching techniques to combat net radio. *Proceedings of the IEEE*, 75(1):43–55, January 1987.

[7] C. R. Davis. *IPSec: Securing VPNs.* Osborne/McGraw-Hill, New York, 2001.

[8] A. Ephremides, J. Wieselthier, and D. Baker. A design concept for reliable mobile radio networks with frequency hopping signaling. *Proceedings of the IEEE*, 75(1):56–73, January 1987.

[9] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of 28th IEEE Symposium on Foundations of Foundations of Computer Science*, pages 427–437, October 1987.

[10] P. Feldman and S. Micali. An optimal algorithm for synchronous byzantine agreement. *SIAM. J. Computing*, 26(2):873–933, 1997.

[11] W. C. Fifer and F. J. Bruno. The low-cost packet radio. *Proceedings of the IEEE*, 75(1):33–42, January 1987.

[12] J. Fischer, J. Cafarella, C. Bouman, G. Flynn, V. Dolat, and R. Boisvert. Wideband packet radio technology. *Proceedings of the IEEE*, 75(1):100–115, January 1987.

[13] I. S. . for Wireless LAN. Ieee std 802.11b-1999, 1999.

[14] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold dss signatures. In *Proceedings of Eurocrypt '96 LNCS*, volume 1070, pages 354–371. Springer-Verlag, May 1996.

[15] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. In *Proceedings of Crypto '95 LNCS*, volume 963, pages 339–352. Springer-Verlag, August 1995.

[16] R. Housley, W. Polk, W. Ford, and D. Solo. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. Internet Request for Comments (RFC 3280), April 2002.

[17] J.-P. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001)*, pages 146–155, October 2001.

[18] J. Jubin and J. D. Tornow. The darpa packet radio network protocols. *Proceedings of the IEEE*, 75(1):21–32, January 1987.

[19] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu. Adaptive security for multi-layer ad-hoc networks. In *Special Issue of Wireless Communications and Mobile Computing*. Wiley Interscience Press, August 2002.

[20] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad hoc networks. In *Proceedings of the 9th International Conference on Network Protocols (ICNP)*, pages 251–260, November 2001.

[21] B. M. Leiner, D. L. Nielson, and F. A. Tobagi. Issues in packet radio network design. *Proceedings of the IEEE*, 75(1):6–20, January 1987.

[22] H. Luo and S. Lu. Ubiquitous and robust authentication services for ad hoc wireless networks. In *Proceedings of 7th IEEE Symposium on Computers and Communications (ISCC '02)*, July 2002.

[23] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 internet public key infrastructure online certificate status protocol - ocsp. Internet Request for Comments (RFC 2560), June 1999.

[24] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Proceedings of Crypto '91 LNCS*, volume 576, pages 129–140. Springer-Verlag, August 1991.

[25] T. P. Pedersen. A threshold cryptosystem without a trusted party. In *Proceedings of Eurocrypt '91 LNCS*, volume 547, pages 522–526. Springer-Verlag, April 1991.

[26] N. Schacham and J. Westcott. Future directions in packet radio architectures and protocols. *Proceedings of the IEEE*, 75(1):83–99, January 1987.

[27] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[28] V. Shoup. Practical threshold signatures. In *Proceedings of Eurocrypt 2000 LNCS*, volume 1807, pages 207–220. Springer-Verlag, May 2000.

[29] F. A. Tobagi. Modeling and performance analysis of multihop packet radio networks. *Proceedings of the IEEE*, 75(1):135–155, January 1987.

[30] L. Venkatraman and D. P. Agrawal. A novel authentication scheme for ad hoc networks. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, volume 3, pages 1268–1273, 2000.

[31] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network Magazine*, 13(6):24–30, November/December 1999.

[32] P. Zimmermann. *The Official PGP User's Guide*. MIT Press, 1995.