CERTIFICATE-BASED AUTHENTICATION IN MANETS: SCENARIO-BASED SIMULATION EXPERIMENTS AND METRICS

[1]E Ravi, Assistant Professor, Mail ID:eslavathravi@gmail.com
[2]G Harika, Assistant Professor, Mail ID:harikagora@gmail.com
[3]Dr M Bal Raju, Professor, Mail ID:drrajucse@gmail.com
College Name: Swamy Vivekananda Institute of Technology
[4]FIRDOSE FATHIMA, Assistant Professor, Mail ID:@gmail.com
Department of CSE Engineering
Pallavi Engineering College Hyderabad, Telangana 501505

ABSTRACT: - In wired networks the certificate-based authentication is well studied. Adapting certificate authentication protocols for motive ad hoc networks (MANETs) is, though, a non-trivial job, primarily because there is generally no set infrastructure or centralized management in a MANET as opposed to traditional wired networks. For example, a traditional authentication scheme based on certificates uses a set trustworthy Certificate Authority (CA) to establish, distribute, renew, and revoke certificates. In the MANET method it is normally not feasible to incorporate such a fixed unified CA in the network due to problems including node versatility, restricted wireless media and regular connection failures. A variety of ways to solve the particular problem of applying certificate-based methods for remote authentication on mobile ad hoc networks is suggested. Our contribution is twofold in this paper. We first analysis the specifications of a protected distributed authentication scheme for MANETs and then review some of the current certificate-based authentication systems, in the sense of distributed authentication, by examining their features including pros and cons. Finally, a set of modeling tests and metrics on the situation was proposed to test these characteristics.

Key Words: -Ad hoc networks and cameras, authentication, measurement, emulation.

1. Introduction

Mobile Ad hoc networks (MANETs), partially due to the possible usage of MANETs in various apps, have gained significantly greater attention. However, the usage of these networks presents many complicated problems because of the complex existence of nodes, the random topology, the restricted wireless range of nodes and communication errors. Since all nodes in the network operate together to relay information, the wireless channel is vulnerable to active and passive attacks by malicious nodes, such as service denial, eavesdropping, spot-spoofing, etc. The design of encryption in these networks is therefore of prime importance.

Confidentiality, honesty, authenticity, availability and non-reputability are the five elements of a protection system. Authenticity is, thus, the most critical question, because an authenticity infringement contributes to a system-wide compromise. The public key management scheme that uses certificates is one of the commonly used authentication methods in traditional wired networks.

The stable delivery of public keys to all nodes in the network is one of the primary problems in a certificate-based framework. The PKI [1] describes public key management methodologies utilizing X.509 certificates. There is a centralized certificate server in a wired network, which is responsible for developing, renovating and revoking certificates. In ad hoc networks, this is not necessary when there is no set framework and unified control. In addition to this, recurrent connection failures can occur due to complex network topology, contributing to issues such as authentication and timely contact with the certificate server.

Several methods for public key management were introduced to address these shortcomings and to take maximum advantage of the certificate authentication mechanism [2]. In this article we examine some of these approaches and address their benefits and drawbacks. The remainder of the document is structured accordingly. Section 2 outlines the criteria for a handheld ad hoc network certificate-based authentication scheme. Section 3 includes an examination and a short summary of the processes employed. Section 4 contrasts the schemes with the specifications. In Section 5, we mention scenarios and methods for the analysis of these processes through simulation.

2. Requirements of effective certificate-based authentication for ad hoc networks

Five specifications have been established to ensure a safe and efficient authentication in a mobile ad hoc network with any certificate-based authentication scheme.

R.1 Disseminated authentication: It is not normally practical to have a fixed centralized CA in the network on ad hoc networks due to problems such as regular connection errors, node mobility and restricted wireless medium. Furthermore, a server may become a single point of vulnerability in networks that need high protection. Consider the war situation, for example, in which the soldiers scatter over a wide region. In such a scenario, a central server could

not be feasible. Consider an adversary server attack - the entire network will fall down! A certificate-based mechanism's primary constraint is to spread authorization across a variety of nodes inside the network.

R.2 Resource sensitivity: Because ad hoc network nodes normally operate on limited memory capacity batteries, the authentication protocols have to be resource-conscious. This ensures there is an appropriate low time and space complexity of the underlying algorithms. In this respect, symmetric-key-based encryption strategies are more suitable, relative to public key approaches, because symmetric encryption typically contributes to fewer use of energy. However, the challenge of sharing the symmetric keys prohibits their usage in ad hoc networks. There is a compromise that needs to be discussed at the implementation stage. Because certificate-based authentication uses resource-intensive public key mechanisms, both the memory and the power of the protocol itself must be effective.

R.3 Effective certificate management mechanism: public keys delivery and certificate management is deeply studied for wired networks [3]. However, the management of certificates (creation, revocation and renewal) is a difficult matter in enforcing these methods for MANETs. Parts 3 and 4 explore this more. Many of the proposed processes ignore a rigorous revoking certificate system.

R.4. R.4. Heterogeneous registration: As in the case of wired networks, often in ad hoc networks the certification authorities may be heterogeneous. This ensures that two or more nodes from separate "domains" will attempt to authenticate each other. In such a situation, the certifying authority must have some sort of confidence arrangement or hierarchy. This is done in wired networks by credential chaining.

R.5. R.5. Robust mechanism for pre-authentication: we mean the method by which the requisite faith is formed between the nodes prior to the development and distribution of the certificate. Although this is not part of the verification of the certificate itself, it is highly necessary in MANETs. This is because it is necessary for nodes to have prior confidence between each other to fulfill R.1 (by exchange of public keys, for example). The subsequent reciprocal authentication and renewal of certificates would not be feasible without this created. Stajano and Anderson's [8] Resurrecting Duckling model was one of the early ventures in this area, which included the bootstrapped confidence between a "mother" and a "pushing-in" node over a local channel. Balkans et al [9] address an accessible and user-friendly solution. The scope of this paper is beyond a thorough classification of these processes.

3. Survey of Related Work

The authentication based on certificates typically consists of three steps. The nodes are given a certificate by a certifying authority during the first step or "bootstrapping" level. The CA produces the certificate with the identification details of the node, such as the IP address, name, organization and public key. In addition to other material, the certificate consists of the problem period and the expiry time. The credential will be "renewed" during the second process prior to its expiry. The third stage includes the revocation of the CA certificate, likely through breaching the certificate holder's private key or probably by believing the issuer that the user's key obligation is no longer legitimate in some way. We are now exploring some of the methods suggested.

3.1. Self organized public key management

One of the authentication procedures suggested by Catkin, Bettina and Hubbub on the basis of certificates is by the creation of graphs [4]. The solution proposed is close to PGP certificates [10], only that a central credential server is used in PGP. A graph is known as a graph directs G (V, E) with V and E representing the set of vertices and the set of edges. The certificate graph vertices are public keys and the edges are certificates. As shown in Figure 1, a directed edge of the graph from Ku to Kava reflects the certificate given by u to v, which is signed with a private key against the Kava public key. In reality, u is the CA for v. G only contains valid network certificates.

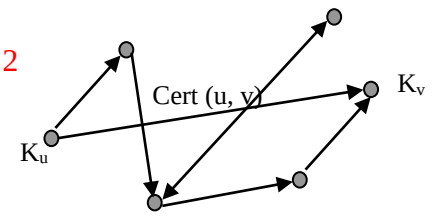

Figure 1: Ku →KV, certificate issued to v by u

Each node maintains a current and un-updated repository of local certificates consisting of a subset of updated and expired certificates. Catkin et al. suggest that two libraries be used to provide a good evaluation of the certificate graph and authentication of the node. Whenever a user u needs to validate the genuineness of another user's public key v, u attempts to find a guided route in the network by combining modified certificate registry graphs u and v. To authenticate v the path is used to balance the chain of certificates. If no path is identified the node merges the un-updated and updated certificate repositories to find the expired certificates in the path. When discovering such a route, the expired certificate is modified; the correctness is verified and authenticated.

Every node creating its own public-private key pairs starts with the certificate development process. The issuer verifies the validity of the public key if a new node demands a new certificate from its neighbor. Catkin et al. presume that the key is pre-exchanged through a side channel. To update the certificate graphs in the updated registry, a certificate exchange process is done regularly by sharing certificate hashing with neighboring nodes. The convergence periods are upper bound until all nodes are modified with the certificate maps. Catkin et al. suggest algorithms such as Maximum Grade algorithms based on the route in certificate charts with the largest number of certificates to optimize the usefulness of the modified certificate registry development and upgrading.

Catkin et al. may not discuss any specific method of renewal of the certificate when a node detects expired certificates in its inundated certificate repository. They recommend two approaches for revoking certificates, one concrete and the other implied. The certificates are withdrawn through the tacit process on the grounds of their expiration period. The issuer specifically sends a cancelation statement to the target node that it does not think a valid user-key binding is any longer valid. This is sent to nodes who seek certificate updates for the target node from the issuer.

The benefit of this system is that public key control is completely self-organized with certificates. But the limitations of the system are the costly tables for credential servers to manage, because any time a node transfers between localities, it must renegotiate with other nodes and refresh the tables again.

3.2. Providing Robust and Ubiquitous Security Support for MANETs

Kong et al [4] are considering a distributed credential focused on thresholds and mutual secrets in this system. The basic purpose of a secret threshold sharing approach is to exchange a secret key k with an arbitrarily large population using a secret polynomial f (x). If f(x) is (k-1), any k group member would be able to retrieve the hidden key, although any members less than k will not share any details about the secret [6]. Therefore, from its k adjacent nodes, a node derives its public key. Here, k is a parameter that must be carefully modified to make the process effective.

The credential generation method is as follows: all nodes in the network must initially be booted by a trustworthy central management with their certificates. If a new node needs to get its certificate, it then sends a submission for partial certificates to its k-neighboring nodes. When the coalition determines that the demanded node is a well-preserved node, it releases its partial certificates, which are merged by the goal of the new certificate with an interpolation feature.

The credential is renewed by stating a Period Renew renewal. A network agency broadcasts the existing valid certificate to its neighbors in the one jump, as well as a potential phrase T < (current time + renew), to update a certificate. The adjacent nodes search the public device key and the credential revocation list to figure out whether the request is approved or denied.

Revocation of the credential is carried out through tacit or formal processes utilizing two approaches, as proposed in [2]. The certificates are cancelled by the tacit method if the expiry period (Expire) is shorter than the expiry time plus the renewal time (Renew). Each node maintains a certificate revocation list of certain certificates which have not yet expired, in the clear certificate revocation protocol. The node routinely consults its CRL on expired certificates and, if appropriate, revokes them.

The fundamental benefit of this approach is that no centralized certification body is needed. However, it relies on a node with at least k one-hop authentication neighbors. This cannot be feasible if k is high because of the complex existence of the nodes. Furthermore, nodes that are more than hop apart cannot be released with the certificates. It also needs a bootstrapping process to initially disperse the system's private key between k nodes.

3.3. Self Managed Heterogeneous Certification

Wang, Zhu and Li [3] suggest a new framework for the co-existence of CAs in the network from separate administrative areas. They also suggest a distributed authority for certificates utilizing a hidden k-threshold exchange close to the Kong et al method [4]. Esteem diagrams are used to treat heterogeneous CAs. A node A is said to have trusted node B if node B can be authentically checked using the digital B certificate signed by the CA that A currently trusts. Each node has a list of trustworthy CAs.
Whenever a node requires a credential, it needs to gather K IDs from its one-hop neighbors of legitimate shareholders and generate a private key. Any time a node a need to authenticate another node B, it starts by giving B its CA list. Likewise, B gives a CA list of its own. A then compares the two lists to look for any common CAs, and if so, A sends its certificate to B which is CA-certified. B responds by submitting a certificate of its own to A. If the two nodes have a shared CA, they continue via the distributed multi-hop certificate request (DMCR) algorithm to check their one-hop and two-hop neighbors.
The certificate renewal phases are identical to the DMCR method. However, the denial of licenses is not addressed.

The key benefits of this method are I cross-certification assistance between ACs in numerous areas; (ii) the discovery process for certificates is carried out in many shops.

3.4. Trust- and Clustering-Based Authentication

Ngami et al [5] address a faith model and a network model in order to strengthen public certification security. Your network architecture is focused on the hierarchical structure or clustering of the network by such clustering algorithms. The authors acknowledge that such algorithms promote network protection and performance. You believe that the network is split into individually named clusters.
Their confidence model is based on the PGP-like web-of-trust model [10], in which each individual will serve as a certifying authority. They quantitatively describe confidence as a constant value between 0 and 1. Each node holds a list of trust values for other network nodes. A direct trust is described as a relationship of trust between two nodes in the same community and a confidence of suggestion, the relationship of trust between nodes of separate classes. To create the confidence bond, the nodes are expected to be fitted with such tracking components such as the surveillance dog for nodes' actions.
Public main control inside a cluster is believed to be present. If a node wishes to authenticate a node in another cluster, it connects with many other nodes in the cluster. It sorts the introductory nodes based on their trust values and determines their weighted trust value by comparing their trust values from the introductory nodes with the trust values of the introductory nodes to the objective node. The final value of the confidence is then saved and used to compare other nodes.

The writers do not discuss a renewal and cancelation process. The drawback of the mechanism is that a significant percentage of malicious nodes may be detected and isolated relative to PGP-based approaches. The downside is that the storage and measurement of the trust values are memory and time-consuming. In addition, node mobility contributes to node membership shifts in multiple clusters.

4. Comparison of the Mechanisms

Table 1 contrasts the four mechanisms with the specifications mentioned above. We may not take into consideration R.5 since it is not an integral aspect of the credential process itself.

Table 1: Comparison of Certificate-based Authentications

Requirements	*Self Organized Public Key Management - Capkun*	*Providing Robust and Ubiquitous Security Support for Mobile Ad hoc Networks – Kong*	*Self Managed Heterogeneous Certification in Mobile Ad Hoc Networks – Wang*	*Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks – Ngai*
R.1. Distributed authentication	It is a totally distributed certification method since every node acts as a CA.	Totally distributed and scales well to large networks	Totally distributed and scales well to large networks	Distributed and self organized since every node acts as a CA
R.2. Resource awareness	Each node maintains two certificate repositories, which incurs a high overhead.	The generation and distribution of keys using complex polynomial functions is resource-intensive and time consuming.	Each node only maintains a list of its trusted CAs. Thus it is more efficient than method proposed in [2].	The maintenance of trust tables and the monitoring components are memory intensive.
R.3.(a) Creation	Self–signed certificates, and hence more robust than a shared key based mechanism	Requires at least k neighbors which might be a bottleneck	Similar to K-threshold mechanism [4]	Across nodes, creation is based on trust values. The existence of introducing nodes may not be true at all times.
R.3.(b) Renewal	No explicit mechanism discussed	Same as issuance	Implemented through the DMCR algorithm	Not discussed
R.3.(c) Revocation	Explicit revocation causes delay between far-away nodes in the network.	System CRL table stored at each node and hence memory intensive.	Not discussed	Not discussed
R.4. Heterogeneous certification	Not implemented.	Not implemented.	Implemented using trust graphs.	Not implemented

5. Scenarios and Metrics

To research the feasibility of these processes, we suggest a variety of practical simulation scenarios. We must first identify certain conditions before deciding the scenarios.

5.1. Parameters for defining the scenarios

1) The mobility model reflects practical network node motions. They can be categorized mostly as mobility models for organizations and mobility models for classes. Camp et al. grant these models a wider classification [11]. The RWM (Random Waypoint Model) is the most popular mobility model for the science group which uses pause periods and random shifts in destinations and speed. Randomness therefore does not well fit some situations, such as an area of war, in which mobility is more predictive. Moreover, over a long simulation time, the model still struggles to provide "statelessness"[12]. Therefore, mobility models should be cautiously selected when testing and authentication method dependent on the credential. The realistic situation must be formed as tightly as possible.

2) The density of nodes often differs based on the case. An incident coverage scenario, for example, may have a high node density, whereas a disaster recovery scenario may have a low density as nodes are distributed over a vast region.

3) Levels of traffic differ based on faults in node links, congestion and mobility. Sources and traffic sort (e.g., CBR, TCP or UDP) must also be addressed as the scenario is specified. The traffic form used is usually the constant bit rate (CBR). For a practical example, a packet rate and size might be 4 packets per sec and 512 bytes respectively.

Table 2 describes sample situations and their corresponding simulation parameters. Scenarios I and II are based on the mobility model (RPGM) of the Reference Point Group [11]. RPGM is a model of community mobility with a rational centre (like a soldier's head) for each group that defines the group behavior. The nodes within a community

shift arbitrarily according to the RWM, but the leader decides the Group's total movement. Scenarios III and IV are focused on templates for agent mobility. The Random Waypoint is the most widely employed object versatility model. However, the Manhattan Grid Concept is used in scenario III for practical situations and the Gauss Markov Model is included in scenario IV.

Table 2: Sample Scenarios

parameters	*I. Battlefield*	*II. Rescue Operation*	*III. City traffic*	*IV. Event Coverage*
Mobility model	RPGM	RPGM	Manhattan Grid	Gauss Markov Model
Number of nodes	10 in each group 5 groups	5 in each group 10 groups	50	50
Area	2000 * 2000 m	1000 * 1000 m	1500 * 500 m	500 * 500 m
Speed	Node speed: 5 m/s Group speed : 1 m/s	Node speed: 2 m/s Group speed : 5 m/s	Node speed: 20 m/s	Node speed: 2 m/s Group speed : 5 m/s

5.2. Metrics

After having specified the scenarios parameters, we have established the following measurements, which can be used to test authentication mechanisms. Any of the measurements were modified from [7].

a) *Successful Certification Ratio* (μ) measures the ratio of the number of successful certification services (including issuance, NC_{ISS}, and renewal, NC_{REN}, respectively) to the total number of requests for such services ($NC_{TOT\text{-}ISS}$ and $NC_{TOT\text{-}REN}$, respectively). It gives an idea about the efficiency of the mechanism in providing successful certification services. If we consider μ_{REN} as the successful certification renewal ratio, and μ_{ISS} as the successful certificate issuance ratio, then their respective value can be calculated as follows:

$$\mu_{REN} = \frac{NC_{REN}}{NC_{TOT-REN}} \qquad \mu_{ISS} = \frac{NC_{ISS}}{NC_{TOT-ISS}}$$

Here, NC_{REN} and NC_{ISS} are the respective total number of certificates renewed and issued, and $NC_{TOT\text{-}REN}$ and $NC_{TOT\text{-}ISS}$ the respective number of requests for certificate issuance and renewal.

b) *Settling time (st)* measures the initial time taken for all the nodes in the network to be issued valid certificates. The value of *st* can be calculated as the difference between the time when all the nodes are issued valid certificates and the starting time when the process of certificate issuance begins. The settling time taken will depend on factors such as the number of malicious or non-cooperative nodes, the algorithms used for key generation and distribution, etc. If the pre-authentication methods are efficient (R.5), the settling time will be less.

c) *Frequency of Certification* (f_{cert}) measures the number of certification services per time interval.

$$f_{cert} = \frac{N_{cert}}{T_{int}}$$

Here N_{cert} is the total number of certification services (issuance/renewal) by nodes in the network, and T_{int} is the simulation time. As the topology of the network changes, it is expected that there will be frequent certificate issuance and renewal processes. This incurs overhead, since each time a node wants to create or renew its certificate costly computations have to be carried out for the public key mechanism. We intuitively predict that a distributed and self-organized mechanism will have a lower frequency of certificate creation, renewal and revocation, and hence, a lower f_{cert}.

d) *Average Certification Delay (acd)* is measured as the time delay between the certificate service request (*CSReq*) and the certificate service reply (*CSRep*) averaged over the simulation time.

$$acd = \frac{\Sigma_{i=1..n}(CS\,\mathrm{Re}\,p_i - CS\,\mathrm{Re}\,q_i)}{T_{int}}$$

This value estimates the efficiency of the algorithm, and mainly depends on the time complexity of the algorithm.

6. Summary and Future Work

Successful authentication in mobile ad hoc nets is crucial for ensuring that the sponsored application runs safely and efficiently, especially in remote field applications where mobile nodes are dispersed around a wide geographical

region. Several security schemes focused on certificates for MANETs have been suggested. We review some of these processes and define certificate authentication criteria for MANETs. We also suggest several theoretical scenarios and measurements that are used in simulation experiments utilizing Network Simulator ns-2[13].

References

[1] Internet X.509 Public Key Infrastructure Certificate and CRL Profile - RFC 2459.

[2] S. Capkun, L. Buttyan and J-P Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc Networks ", IEEE Transactions on Mobile Computing, Vol. 7, No. 1, Jan-Mar 2010, pp. 52-64

[3] Weihong Wang, Ying Zhu, Baochun Li. "Self-Managed Heterogeneous Certification in Mobile Ad Hoc Networks ", in the Proceedings of IEEE Vehicular Technology Conference (VTC 2003), Orlando, Florida, 10/6-9, 2011.

[4] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. "Providing robust and Ubiquitous Security support for Mobile Ad Hoc Networks ", Proceedings of the 9th International conference on Network Protocols (ICNP), Riverside, California, USA, November 11-14 2012.

[5] Edith C. H. Ngai and Michael R. Lyu. "Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks", 24th International Conference on Distributed Computing Systems Workshops - W4: MDC (ICDCSW'04), Hachioji, Tokyo, Japan, 3/23-24, 2004.

[6] L. Zhou and Z. Haas. "Securing Ad Hoc Networks", IEEE Network magazine, special issue on networking security, Vol. 13, No. 6, November/December 1999.

[7] Matei Ciobanu Morogan, Sead Muftic. "Certificate Management in Ad Hoc Networks", 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), January 27 - 31, 2003, pp. 337.

[8] F. Stajano and R. J. Anderson. "The resurrecting duckling: Security issues for ad-hoc wireless networks" In 7th Security Protocols Workshop, volume 1796 of Lecture Notes in Computer Science, Cambridge, United Kingdom, 1999. Springer-Verlag, Berlin Germany.

[9] Dirk Balfanz, D. K. Smetters, Paul Stewart and H. Chi Wong: "Talking To Strangers: Authentication in Ad-Hoc Wireless Networks", Symposium on Network and Distributed Systems Security (NDSS'02), Xerox Palo Alto Research Center, Palo Alto, USA, 2002.

[10] P. Zimmerman. The Official PGP Users guide, MIT Press, 1995, ISBN 0-262-74017-6.

[11] T. Camp, J. Boleng, and V. Davies. "A Survey of Mobility Models for Ad Hoc Network Research", in Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, vol. 2, no. 5, 2002.

[12] J. Yoon, M. Liu, and B. Noble. "Random waypoint considered harmful," in Proc. of IEEE INFOCOM '03, vol. 2, March 2003, pp. 1312—1321.

[13] K. Fall and K. Varadhan, the NS Manual, the VINT Project, UC Berkeley, January 2002.

