Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 11 Version 1.0 June 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Wireless Adhoc Networks Security Principles, Issues & Applications

By Ramesh Kait, Kuldeep Kherwal & C. Nelson Kennedy Babu
Singhania University Rajsthan

Abstract - Privacy and integrity of packets on WANetworks should be expected by the algorithmic mechanisms. This privacy and integrity is very much is to be mandated by regulations. In tradition the security is only based on cryptographic techniques which is not so much secure and leads to unsecure and unauthenticated information. As the packets of information are to be routed on networks so it needs some new security and digital signature based algorithm. A digital signature method provides the solution to many of these new concerns. So in this paper we will discuss new paradigm of digital signature based techniques along with merit & demerits, applications and issues related with it.

Keywords : *Digital Signature,Cryptography, Security, RSA , Hash Function.*

GJCST-E Classification: *C.2.1*

Strictly as per the compliance and regulations of:

Wireless Adhoc Networks Security Principles, Issues & Applications

Ramesh Kait [α], Kuldeep Kherwal [σ] & C. Nelson Kennedy Babu [ρ]

Abstract - Privacy and integrity of packets on WANetworks should be expected by the algorithmic mechanisms. This privacy and integrity is very much is to be mandated by regulations. In tradition the security is only based on cryptographic techniques which is not so much secure and leads to unsecure and unauthenticated information. As the packets of information are to be routed on networks so it needs some new security and digital signature based algorithm. A digital signature method provides the solution to many of these new concerns. So in this paper we will discuss new paradigm of digital signature based techniques along with merit & demerits, applications and issues related with it.

Keywords : Digital Signature, Cryptography, Security, RSA, Hash Function.

I. Introduction

With the advent of wireless network as packet radio networks in the 1970's, it became an interesting research subjects in computer world [1, 2, 5, 7, 12], and in these three fold decades tremendous improvement is made in the research. Wireless adhoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). Wireless communication devices, could form an ad hoc network when they roam in a battlefield. Wireless networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

II. Issues of Security

As security is a complex objective, in order to achieve this objective, the issues is to be clearly defined:

- **Authentication:** Are user who they say they are?
- **Access Privileges:** What applications and information can a particular user read, writes, or modify?
- **Accountability:** Did the person responsible for the information?
- **Traceability:** What is the change and review history of the information?

There can be a sure attack on the wireless adhoc network system because the attackers always think a one step ahead to the network designer, so there must be some security design to achieve the security objective.

III. Concept of Secure System Model

In order to maintain the security of wireless adhoc network using digital signature technique is very much suitable because it is based on mathematical formula and enables the unauthenticated person to break it very hard. A **digital signature/Scheme** is a mathematical scheme [5, 6, 8, 9] for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery/Tempering.

IV. Encryption for Privacy

Encryption refers to algorithmic schemes that encode plain text into non-readable form or Cipher text, providing privacy. The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form. The key is the trigger mechanism to the algorithm.

Until the advent of the Internet, encryption was rarely used by the public, but was largely a military tool. Today, with online marketing, banking, healthcare and other services, even the average householder is aware of encryption.

There are many types of encryption and not all of it is reliable. The same computer power that yields strong encryption can be used to break weak encryption schemes. Initially, 64-bit encryption was thought to be quite strong, but today 128-bit encryption is the standard with DES Schemes, and this will undoubtedly change again in the future. The **figure1.0** gives the process of the scheme how it works. There can be the two techniques of Cryptography can be used the description is as bellows

General Description of Symmetric (Private Key) Cryptography also known as most popular Symmetric

Author α : Department of Computer Science & Applications Kurukshetra University Kurukshetra. E-mail : rameshkait@kuk.ac.in
Author σ : Research Scholar, Singhania University Rajasthan. E-mail : ks.kherwal@gmail.com
Author ρ : PG Computer Science & Engineering,Shri Sowdambiga College of Engineering, Aruppukottai,Tamilnadu. E-mail : cnkbabu63@yahoo.in

Key is also known as DES i.e. Data Encryption Standard is as

- *k* is the key agreed on beforehand by A and B
- *m* is the message to be sent from A to B
- *Ek* is the encryption algorithm using key *k*,
- *Dk* is the decryption algorithm using key *k*

A sender encrypts message *M* using *Ek* (*m*) and sends it to B Receiver,

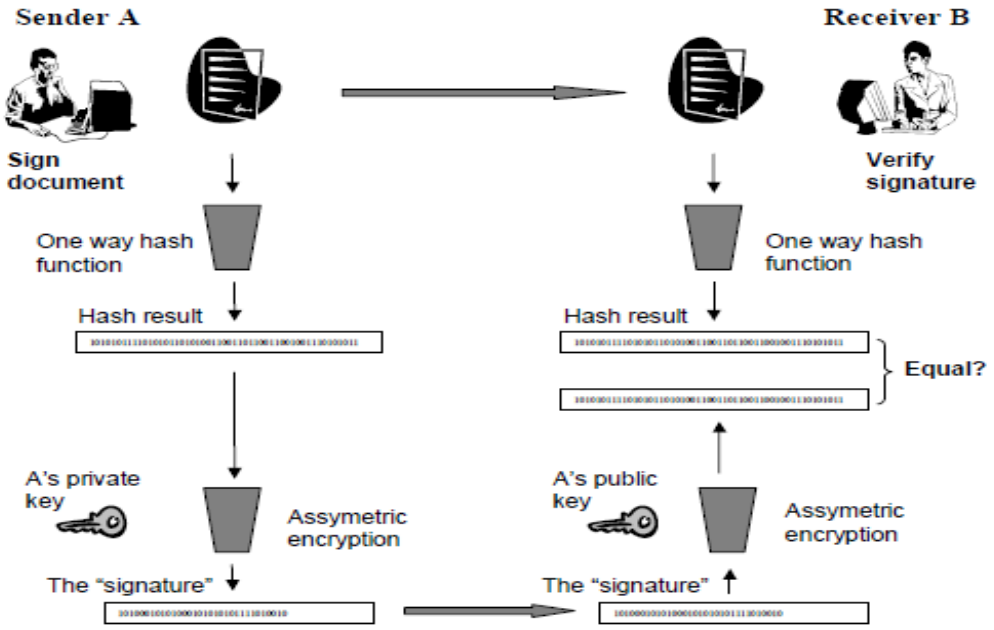

Fig. 1.0 : Digital Signature Processing Scheme

B decrypts using *Dk* (*Ek* (*m*)) and recovers the message *M* & incase of the Asymmetric (Public Key) Cryptography

- *m* is the message to be sent from A and B,
- *Eb* is the encryption algorithm using B's public key,
- *Db* is the decryption algorithm using B's private key.

A sender encrypts the message *m* using *Eb* (*m*) and transmits the results to B,

B decrypts using *Db* (*Eb* (*m*)) and recovers the message *m.*

As the above figure 1.0 shows that the digital signature is formed in two ways. First, A computes the hash value of her message; next, she encrypts the hash value with her private key. Upon receipt of the digital signature, B recovers the hash value calculated by A by decrypting the digital signature with A's public key. B can then apply the hash function to A's original message, which he has already decrypted. If the resultant hash value is not the same as the value supplied by A, then B knows that the message has been altered; if the hash values are the same, B should believe that the message he received is identical to the one that A sent.

This scheme also provides Non repudiation since it proves that A sent the message; if the hash value recovered by B using A's public key proves that the message has not been altered, then only A could have created the digital signature. B also has proof that he is the intended receiver; if he can correctly decrypt the message, then he must have correctly decrypted the session key meaning that his is the correct private key. Symmetric key (also called private key or secret key) cryptography [7, 8] uses the same key to encrypt and decrypt. The name "private key" derives from the need to keep the key private. A major challenge associated with symmetric key cryptosystems is the secure distribution of keys. Asymmetric key encryption (also called public key encryption) uses two keys: a public and a private key. Data encrypted with one key can be decrypted only with the other key. Asymmetric cryptography solves the challenge of secure distribution of secret keys.

Anyone with the public key can use it to perform a validity check of digital signatures created by the private key. Only a digital signature created by the appropriate private key decrypts and validates properly with the public key. If a different private key was used to sign the data, the validity check fails. If the contents of digitally signed data or the digital signature have been tampered with or are corrupted, the validity check also fails. Valid digital signatures can be used to perform the following functions:

1st Authenticate online entities, 2nd Verify the genuineness or origin of digital data and, 3rd Ensure the integrity of digital data against tampering.

Advantage of Digital signature is eliminating the possibility of committing fraud by an imposter signing since the digital signature cannot be altered, this makes forging the signature impossible. Beside this it helps in legal requirement and message integrity also. But implementation of this scheme is costly.

Disadvantage of encrypting all data to provide a digital signature is impractical for three reasons:

- The cipher text signature is the same size as the corresponding plaintext, so message sizes are doubled, consuming large amounts of bandwidth and storage space.
- Public key encryption is slow and places heavy computational loads on computer processors, so network and computer performance can be significantly degraded and to overcome these issues we use Digital signature using RSA.

V. Hash Function

A hash function takes a block of data, generally called the message, and returns a fixed-size string, which can be called the hash, hash value or message digest. The main reason for creating a hash value of a message is that any accidental or intentional change to it will result in a completely different hash value. Hashes are not unique. A good hash function should produce message digests that are impossible to brute force in a reasonable amount of time. The hash function should also have statistically evenly distributed collisions. This is called strong collision resistance.

Some properties of a good cryptographic hash function are:

- It is easy to compute the hash value for any given message.
- It is very difficult to find a message that has a given hash.
- It is also very difficult to modify a message without the hash being changed.
- It is not possible to find two different messages with the same hash.
- It can apply to any block size of data.
- It should produce a fixed-length of output data

Hash algorithms that are in common use today are:

- *Message Digest (MD) algorithms:* A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.
- *Secure Hash Algorithm (SHA):* Algorithm for NIST's Secure Hash Standard (SHS). SHA-1 produces a 160-bit hash value
- *RIPEMD :* A series of message digests and 128-bit hash functions.
- *HAVAL (Hash of Variable Length) :* a hash algorithm with many levels of security. It can create hash values that are 128, 160, 192, 224, or 256 bits in length.
- *Whirlpool :* A relatively new hash function .It operates on messages less than 2^{256} bits in length, and produces a message digest of 512 bits.

VI. One Way Hash Function

The main role of hash function is in provision of digital signature. Hash functions are faster than digital signature. One-way chains are an important cryptographic primitive in many security applications. As one-way hash functions are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature [1]. A one way function is a mathematical function that is significantly easier to perform in one direction .Despite the computational efficiency of one-way functions, one-way hash function is still challenging to use in resource-constrained environments, such as on small mobile devices or sensor networks. Especially some of the proposed sensor networks have significant resource limitations, as they use minimal hardware to lower the energy consumption [2]. Generally all modern hash algorithms produce hash values of 128 bits and higher .Sometime called Trapdoor functions also.

VII. Fully Hash Function

The Full Domain Hash (FDH) is an RSA-based signature [9, 12, 13] scheme that follows the *hash-and-sign* paradigm. It is more secure than one way hash function. In the RSA digital signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data. To verify the contents of digitally signed data, the recipient generates a new message digest from the data that was received, decrypts the original message digest with the originator's public key, and compares the decrypted digest with the newly generated digest. If the two digests match, the integrity of the message is verified. The identity of the originator also is confirmed because the public key can decrypt only data that has been encrypted with the corresponding private key. RSA rely upon ``Key Certification Authority'' (CA) that is responsible for issuing and/or certifying keys. The primary role of a key certification authority is to provide assurance that a user's public key is accurate. It is used in most of applications around the world.

Advantage of RSA is that it can recover the message digest from signature.

Disadvantage of RSA is that, it's a time consuming process and create a problem when M> n situation arise, where M is message and n is Block length.

For resolve this problem we should use Hash and sign at a time. There are several reasons to sign such a hash (or message digest) instead of the whole document.

- *For efficiency:* The signature will be much shorter and thus save time since hashing is generally much faster than signing in practice.
- *For compatibility:* Messages are typically bit strings, but some signature schemes operate on other domains (such as, in the case of RSA, numbers modulo a composite number N). A hash function can be used to convert an arbitrary input into the proper format.
- *For integrity*. Without the hash function, the text "to be signed" may have to be split (separated) in blocks small enough for the signature scheme to act on them directly. However, the receiver of the signed blocks is not able to recognize if all the blocks are present and in the appropriate order.

RSA is used in verification than signing because RSA public exponent is usually smaller than RSA private exponent. this is desirable because a message is signed by individual only once but check for verification several times .hence , RSA signature verification is faster .RSA allow both the public and private key to be used for encryption. If a message is encrypted with someone's private key it can only be decrypted with the corresponding public key. This feature can be used to create digital signatures

VIII. Proposed Plan for Security Mechanisms

We proposed solution for the authenticated broadcasting in wireless network to achieve many security goals for many applications that has to be achieved. Some of the measures that can be incorporated are:

- **One way Hash Function:** it is like checksum of a block of text and is secure in, that it is impossible to generate the same hash function value without knowing the correct algorithm and key. It should use for generate digital fingerprints and for encrypt password for operating system.
- **FDH (Full hash function):** FDH is a RSA based signature scheme included hash and sign at a time and use key certification authority for key management.
- **Digital Signature:** External attack can be checked using confidentiality of routing information and also by authentication and integrity assurance features. Digital signature is used for protecting data form compromised nodes.

IX. Conclusion

Hash functions, for example, are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence. The value of hash function is should be long enough to protect attacks. Secret key cryptography, on the other hand, is ideally suited to encrypting messages, thus providing privacy and confidentiality. The sender can generate a *session key* on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message. Asymmetric schemes can also be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography. In last , we suggest for Hash and RSA scheme combination. Further improvement is PKI public key infrastructure is key management to ensure safe public key i.e. signature verification key. It improves WANetworks system effectiveness and efficiency and is the solution for the problem, how to ensure public key signature verification.

X. Bibliography

1. M. Brown, D. Cheung, D. Hankerson, J. Hernandez, M. Kirkup, and A. Menezes. PGP in constrained wireless devices. In Proceedings of the 9th USENIX Security Symposium, pages 247-261. USENIX, August 2000.
2. J. M. Kahn, R. H. Katz, and K. S. Pister, "Mobile networking for smart dust", In ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, WA, August99.
3. Weimerskirch A, Westhoff D, "Zero common-knowledge authentications for pervasive networks" In: Selected Areas in Cryptography. (2003) 73–87
4. O'Shea G, Roe M, "Child-proof authentication for mipv6 (cam)" SIGCOMM Computer. Communication Rev. 31 (2001) 4–8
5. Montenegro, G., Castelluccia, C, "Statistically unique and cryptographically verifiable (sucv) identifiers and addresses" In: Proceedings of the Network and Distributed System Security Symposium (NDSS). (2002)
6. Shamir, A, "Identity-based cryptosystems and signature schemes" In: Proceedings of CRYPTO '84, Springer-Verlag (1984) 47–53

7. Boneh, D., Franklin, M, "Identity-based encryption from the weil pairing" In: Proceedings of CRYPTO 2001, Springer-Verlag (2001) 213–229
8. Cocks, C, "An identity based encryption scheme based on quadratic residues" In: Proceedings of IMA 2001, Springer-Verlag (2001) 360–363.
9. Jochen Schiller. , Mobile Communications, Addison-Wesley 2000.
10. Krishna Moorthy Sivalingam, "Tutorial on Mobile Ad Hoc Networks", 2003.
11. Elizabeth M. Royer and Chai-Keong Toh, "A review of current routing protocols for adhoc mobile wireless networks" Technical report, University of California and Georgia Institute of Technology, USA, 1999.
12. Mobile Ad Hoc Networking Working Group – AODV, http://www.ietf.org/rfc/rfc3561.txt
13. Mobile Ad Hoc Networking Working Group – DSR, http://www.ietf.org/rfc/rfc4728.txt.