International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 10 (October '2016)

ANALYSIS OF RSA SEURITY ARCHITECTURE IN WIRELESS SENSOR NETWORK

S.Sasipriya,
M.Phil Scholar,
Department of Computer Science,
Shri Sakthikailassh Women's College,
Salem,Tamilnadu,India.

R.Umamaheswari,
Assistant Professor,
Department of Computer Science,
Shri Sakthikailassh Women's College,
Salem,Tamilnadu,India.

Abstract: Providing desirable data security, that is, confidentiality, authenticity, and availability, in wireless sensor networks (WSNs) is challenging, as a WSN usually consists of a large number of resource constraint sensor nodes that are generally deployed in unattended/hostile environments and, hence, are exposed to many types of severe insider attacks due to node compromise. Existing security designs mostly provide a hop-by-hop security paradigm and thus are vulnerable to such attacks. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. This 128 bit Encryption algorithm uses 16 characters as secret keys. Public key is used for encryption. Private Key is used for decryption. The value got from the user is converted to bytes and mathematical calculation performed.

Keywords: Wireless sensor network, RSA Algorithm, Encryption, decryption

I.INTRODUCTION

Wireless communication is the exchange of data between two or more points that are not joined by an electrical transmitter. The most well-known wireless technologies use electromagnetic wireless telecommunications, for example, radio. With radio waves distances could be short, for example, a couple of meters for TV remote control, or the extent that thousands or even a huge number of kilometers for profound space radio communications. It includes different sorts of fixed, mobile and portable applications, including two-way radios, cell phones, individual PDAs, and wireless networking [1]. Security in sensor networks is as much an important factor as performance and low energy consumption in many applications. Security in a sensor network is very challenging as WSN is not only being deployed in battlefield applications but also for surveillance, building monitoring, burglar alarms and in critical systems such as airports and hospitals. The sensor nodes are present outside the building so it must protect from the physical changes such as raining, temperature etc. Since sensor networks are still a developing technology, researchers and developers agree that their efforts should be concentrated in developing and integrating security from the initial phases of sensor applications development; by doing so, they hope to provide a stronger and complete protection against illegal activities and maintain stability of the systems at the same time.

a) Types of security attack:

There are two types of security attack are present active attack and passive attack.

1. Active attack in which the attacker cause modification of data. There is physical damage in the network like modification of resources, alteration of data, changing traffic direction or stoppage of data to sink nodes. These attacks are easily identifiable and can stop the attackers as well as start the system recovery process.

There are four categories of active attacks are present masquerade, replay, modification of messages, and denial of service.

- A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- The messages means that some portion of a message is altered or those messages are delayed or reordered, to produce an unidentified effect is called modification attack.
- The denial of service will consume resource of network for unwanted operation. The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target, as a result the entire network either by disabling the network or by overloading it with messages so as to degrade performance [2].

2. Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The goal of this is to obtain information that is being transmitted [3].

b) Security Requirements

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include[4]:

- Availability, which ensures that the desired network services are available even in the presence of denial-of-service Attacks
- Authorization, which ensures that only authorized sensors can be involved in providing information to network services
- Authentication, which ensures that the communication from one node to another node is

genuine, that is, a malicious node cannot masquerade as a trusted network node
- Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired Recipients
- Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate Nodes
- Nonrepudiation, which denotes that a node cannot deny sending a message it has previously sent
- Freshness, which implies that the data is recent and ensures that no adversary can replay old messages Moreover, as new sensors are deployed and old sensors fail,

We suggest that forward and backward secrecy should also be considered:

- Forward secrecy: a sensor should not be able to read any future messages after it leaves the network.
- Backward secrecy: a joining sensor should not be able to read any previously transmitted message. The security services in WSNs are usually centered around cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use.

II.LITERATURE REVIEW

Yi Xiaolin; Chen Nanzhong; Jia Zhigang; Chen Xiaobo, This paper briefly introduces the history of RSA generation and characteristics, the mathematics theories and the basic principles of RSA algorithm. The design and implementation of the trusted communication system based on RSA authentication are described. Then the paper compares the Trusted Communication System with QQ and MSN in performance, safety and speed. Finally the strength of the system and its prospects of application are summarized.

Koji Nakano, Kensuke Kawakami, the main contribution of this paper is to present efficient hardware algorithms for the modulo exponentiation P^E mod M used in RSA encryption and decryption, and implement them on the FPGA. The key ideas to accelerate the modulo exponentiation are to use the Montgomery modulo multiplication on the redundant radix-64 K number system in the FPGA, and to use embedded 18 times 18-bit multipliers and embedded 18 k-bit block RAMs in effective way.

Our hardware algorithms for the modulo exponentiation for R-bit numbers P, E, and M can run in less than (2R + 4)(R/16 + 1) clock cycles and in expected (1.5R + 4)(R/16 +1) clock cycles. We have implemented our modulo exponentiation hardware algorithms on Xilinx VirtexII Pro family FPGA XC2VP30-6. The implementation results shows that our hardware algorithm for 1024-bit modulo exponentiation can be implemented to run in less than 2.521 ms and in expected 1.892ms

Tzer-Shyong Chen; Fuh-Gwo Jeng, Mounting popularity of the Internet has led to the birth of instant messaging, an up-and-coming form of Internet communication. Instant messaging is very popular with businesses and individuals since it has instant communication ability. As a result, Internet security has become a pressing and important topic for discussion. Therefore, in recent years, a lot of attention has been drawn towards Internet security and the various attacks carried out by hackers over the Internet. People today often handle affairs via the Internet. For instance, instead of the conventional letter, they communicate with others by e-mails; they chat with friends through an instant messenger; find information by browsing Websites instead of going to the library; perform e-commerce transactions through the Internet, etc. Although the convenience of the Internet makes our life easier, it is also a threat to Internet security. For instance, a business email intercepted during its transmission may let slip business confidentiality; file transfers via instant messengers may also be intercepted, and then implanted with backdoor malwares; conversations via instant messengers could be eavesdropped. Furthermore, ID and password theft may lose us money when using Internet bank service. Attackers on the Internet use hacking tricks to damage systems while users are connected to the Internet. These threats along with possible careless disclosure of business information make instant messaging a very unsafe method of communication for businesses. The paper divides hacking tricks into three categories: (1) Trojan programs that share files via instant messenger; (2) phishing or fraud via e-mails; and (3) fake Websites

A. Nenadic N. Zhang and Q. Shi , proposed a new cryptographic primitive, called Verifiable and Recoverable Encryption of Signature VRES. Based on RSA-based VRES, they presented two variant protocols RSA-CEMD1 and RSA-CEMD2 for certified e-mail delivery with RSA receipts. They claimed that the protocols provided strong fairness to ensure that the recipient receives the e-mail if and only if the sender receives the receipt. Later, N. Zhang, Q. Shi, M. Merabti, and R. Askwith presented a practical and efficient fair document exchange protocol based on a verifiable and recoverable encryption of keys that is somewhat similar to the VRES. In this paper, we find that the VRES scheme is universal forgeable. Anyone can generate the false VRES for any message without the knowledge of any private key of the sender, the recipient and the TTP. It follows that the two variant protocols RSA-CEMD1, RSA-CEMD2 are all insecure. Meanwhile, we show that the document exchange protocol is not fair since the verifiable and recoverable encryption of keys is not recoverable.

Yanjun Zuo and Brajendra Panda , network viruses", which refer to those viruses spreading through networks. Security attacks can come from both viruses and hacking programs. A network virus makes use of networking protocols and/or applications to spread. We surveyed several hundreds of computer viruses and classified them based on their spreading and infecting mechanisms. Virus intelligence is introduced to describe the various levels of implementing complexity and infecting abilities of network viruses.

Network viruses make uses of system network mechanisms, search local and remote system information, monitor

network traffic, take advantage of system and network vulnerabilities, and build network connections. Intensive network hacking techniques could be borrowed in network virus implementations and both system and network vulnerabilities could be taken advantage of. There are advantages to incorporate hacking abilities into viruses over hacking directly.

III. RSA ALGORITHM

RSA is an encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browser from Netscape and Microsoft, and many other products. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The basic security in RSA comes from the fact that, while it is relatively easy to multiply two huge prime numbers together to obtain their product, it is computationally difficult to go the reverse direction: to find the two prime factors of a given composite number. It is this one-way nature of RSA that allows an encryption key to be generated and disclosed to the world, and yet not allow a message to be decrypted. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. This 128 bit Encryption algorithm uses 16 characters as secret keys. Public key is used for encryption. Private Key is used for decryption. The value got from the user is converted to bytes and mathematical calculation performed. Then public key is applied on the data to have encrypted from and private key is used for decryption process.

Private Key is a mathematical key that can be shared safely so that others can send you encrypted information that only your private key can unscramble. The public key can also verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

In a Public Key Cryptography system, used to decrypt incoming messages and sign outgoing ones. A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

KEY GENERATION ALGORITHM

1. Generate two large random primes, p and q, of approximately equal size such that their product $n = pq$ is of the required bit length, e.g. 1024 bits. [See note 1].
2. Compute n = pq and (φ) phi = (p-1) (q-1).
3. Choose an integer e, 1 < e < phi, such that gcd (e, phi) = 1. [See note 2].
4. Compute the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi). [See note 3].
5. The public key is (n, e) and the private key is (n, d). The values of p, q, and phi should also be kept secret.

Where, n is known as the modulus , e is known as the public exponent or encryption exponent., d is known as the secret exponent or decryption exponent.

Encryption

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m [see note 4].
3. Computes the cipher text $c = m^{\wedge e} \bmod n$.
4. Sends the cipher text c to B.

Encryption Process

Encryption is the process of converting the plaintext to cipher text, to converts 8-bits at time. The Encryption processes are the following:

1. An 8-byte IV is initialized to a value that is different for every plaintext Stream.
2. The IV is encrypted to produce an 8-byte shift register.
3. The first 8-bit of plaintext are XORed with the left most 8-bit in the shift Register to produce the 8-bits of the cipher text.
4. The shift register is shifted 8-bits to the left and the last 8-bits of cipher Text is shifted in to the right most 8-bits of shift register.
5. The shift register is encrypted.
6. The next 8-bits of Plaintext are XORed with the left most 8-bits in the Shift register to produce the next 8-bits of cipher text.
7. Steps 4 through 6 are repeated until all plaintext as been encrypted.
8. The previous steps allow 8-bits of plaintext to be encrypted at a time.

Decryption

Recipient B does the following:-

1. Uses his private key (n, d) to compute $m = c^{\wedge d} \bmod n$.
2. Extracts the plaintext from the integer representative m.

Decryption Process:

Decryption the process of converting the cipher text to plaintext, to converts 8-bits at time. The Decryption is a reverse process of the encryption. And the decryption processes are the following:

1) An 8-byte IV is initialized to the same value used for Decryption and then decrypted to produce an 8-byte shift register.
2) The first 8-bits of cipher text are XORed with the left most 8-bits in the shift register to produce the first 8-bits of plaintext.
3) The shift register is shifted 8 bits to the left, and the last 8 bits of cipher text are shifted in to the rightmost 8 bits of the shift register.
4) The shift register is encrypted.
5) The next 8 bits of cipher text are XORed with the leftmost 8-bits in the left most 8-bits of plaintext.
6) Steps 3 through 5 are repeated until all cipher text has been decrypted.

IV.PROCESS OF RSA AUTHENTICATION ALGORITHM

Suppose that before sending the messages to B, A firstly uses his private key to encrypt the messages, and B uses A's public key to decrypt the messages. Because only A's

e-ISSN: 2395-5325

private key can be used to generate encrypted messages, so the messages can be used for authenticating data source and data integrity. RSA algorithm is certified by the two operations,

$$Y = E\ (PRa, X)$$

And

$$X = D\ (PUa, Y)$$

(PRa is A's private key, PUa is A's public key)

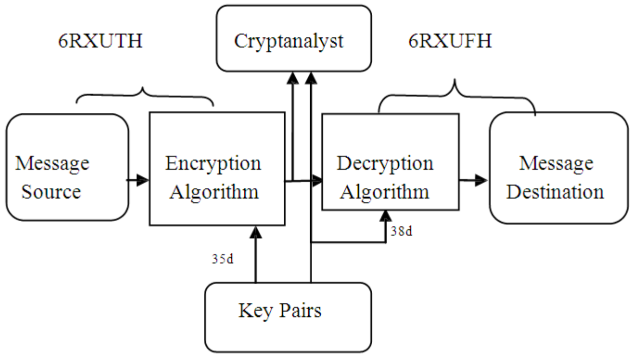


Figure 1: The Process of RSA Algorithm Authentication

V.MODULES

Hacking Disruptor with reliable communication system consists of the following four major modules:

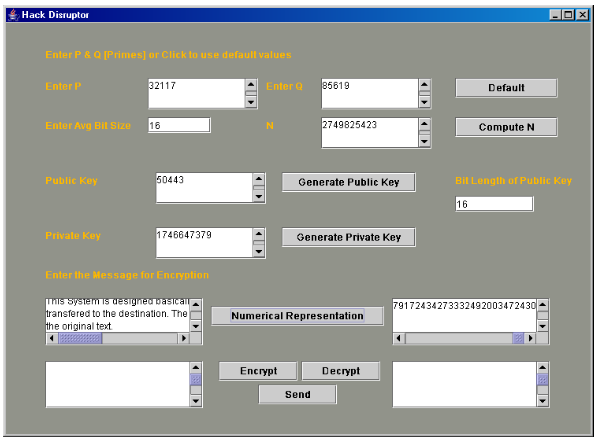
Compute Largest Prime Number: In this module the largest prime number is calculated using the RSA 128 algorithm. The algorithm generates two largest prime numbers. This module takes no input but returns two largest prime numbers.

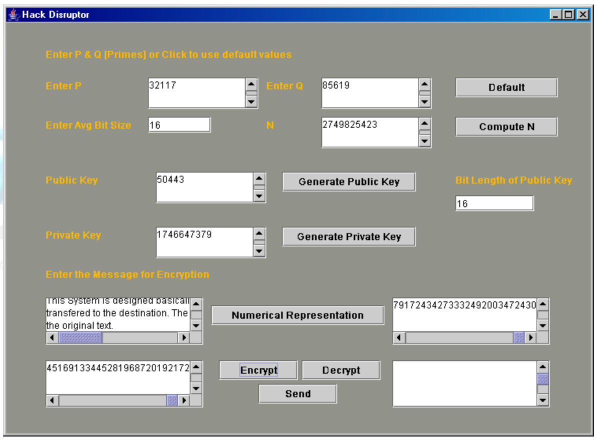
Compute Private and Public Key: This module takes the two largest prime numbers from the previous module as input and computes public and private key. The secret key in a Public Key Cryptography system, used to decrypt incoming messages and sign outgoing ones. A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key. Private key is a mathematical key that can be shared safely so that others can send you encrypted information that only your private key can unscramble. The public key can also verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

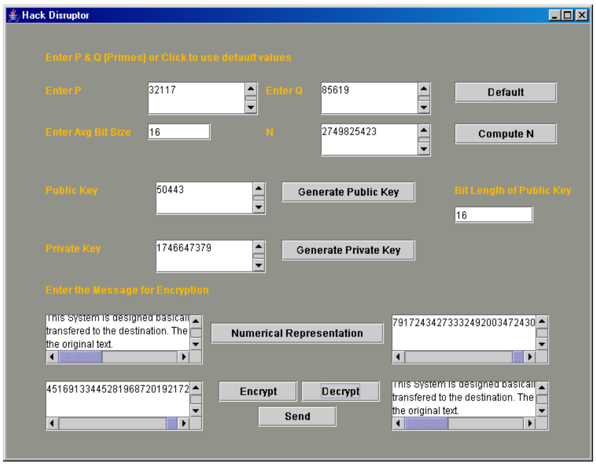
Encryption while transmitting: This module deals with encrypting the data from its original form. Encryption is the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it was not intended, including those who can see the encrypted data. Encryption is sometimes described as the process of converting plain text into cipher text.

Decryption while receiving: The process involves converting encrypted data back into its original form, so it can be understood. To easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on communications without access to the key.

EXPERIMENT OUTPUTS







VI.CONCLUSION

This Proposed system is more flexible than the existing one. Here the text can be encrypted using the private and public

key and is sent to the clients. The text is encrypted, so lacking is not possible. On the receiving and the cipher text is decrypted and the original text is got. The authorized access is not possible in the proposed system. The proposed system is more user-friendly and flexible. It is developed such that all the demerits of the existing system are eliminated. Advantages:The software can be used to Encrypt/ Decrypt files in any platform, The Encryption/ Decryption can be performed for formatted document also, easy to work with the algorithm and Test interface to check out the statistics of the algorithm.

REFERENCES

[1]. http://securityuncorked.com/2008/08/history-of-wireless-security/.
[2]. D. Murat, and S. Youngwhan, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006.
[3]. V. PRAMO, Md. Abdul Azeem, M. OM PRAKASH "Detecting the Sybil Attack in Wireless Sensor Network", International Journal of Computers & Technology, ISSN: 2277-3061 Volume 3, No. 1, AUG, 2012.
[4]. R.L.Rivest, A.Shamir and L.Adleman (1978), "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Comm.ACM, Vol.21 (2), pp. 120-126.
[5]. Ying-yu Cao, Chong Fu (2008), "An efficient implementation of RSA digital signature algorithm", Piscataway, NJ, USA, pp. 100-103.
[6]. LIU Chuan-ling, FAN Jian-hua (2008),"Application of RSA Asymmetrical Encryption Algorithm in Digital Signature", Communication Technology, Vol .42, pp.192-196.
[7]. D.Boneh, H.Shacham (2002), "Fast Variants of RSA,"R.RSA Laboratories Crypto bytes, Vol.5, pp. 1-8.
[8]. J-1. Quisquater and C. Couvreur (1982), "Fast deciphennent algorithm for RSA public-key cryptosystem,"1. Eletronic Letters, vol 18, pp.905-907,
[9]. C .Castelluccia, E. Mykletun, and G. Tsudik (2006). "Improving secure server perfonnance by re-balancing SSLffLS handshakes,"C. Proc of the 2006 ACM
[10]. Symposium on Information, computer and communications security. New York: ACM, pp 26-34.