Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Encryption Scheme for Securing Wireless Network

Ashok Kumar
DAV College Ambala City,
Haryana, India

Abstract*— Many organizations are now considering deployment of ad hoc networks and are working on the basic network designs before going to pilot projects. As always, network security is a concern. The problems with security on these networks have been widely reported elsewhere. Network architects are now faced with the challenge of designing secure networks in light of the known problems. This paper proposes an efficient algorithm for Packet Encryption as well as the standard to detect any kind of intercept attempt. It highlights various cryptographic techniques and suggests a cryptographic technique based on XOR logic gate, which can be used as insulation to packet and detect the interceptions.

***Keywords*— wirless , networks, ad hoc, security, solutions**

I. INTRODUCTION

A recent trend in ad hoc network routing is the reactive on-demand philosophy where routes are established only when required. Mobile Internet connectivity is the fastest growing business in the telecommunications market because of the evolution of digital cellular, portable computing and personal communication technologies. It is playing a vital role in shaping the 21st century communications paradigms. So service demands in wireless communications have significantly changed. The traditional focus was commonly limited to voice channels over wireless point-to-point connections between the base station and the wireless terminal/phone, thus not requiring any complex routing or switching networking topologies. With the introduction of mobile data services, the emphasis shifts from sheer coverage to the flexibility and functionality of the network. A large number of the current wireless service applications require broadband data communications as well as advanced wireless networking services. These advanced services require a new generation network architecture that is powerful and yet flexible enough to enable fast change. With the advent of Globalization, the Business as well as defense applications need highly secured and consistent architecture so that packets can be transmitted in the network without any risk. Trust is the groundwork of the relationship which is established by a business organization with their customers, vendors, and networking. In order to achieve security and privacy in wireless sensor networks, it is necessary to implement and deploy a certain number of mechanisms [2]. Major security issues are: Easy access, Rogue Access Points, unauthorized use of service, MAC Spoofing and Session Hijacking and eves dropping etc.

An attempt has been made to introduce a new algorithm for security. Rest of the paper is organised as follows; section II gives security concerns, Section III defines existing solutions, proposed algorithm is in section IV and last section provides results.

II. SECURE ROUTING

The routing protocols with in ad hoc networks are more vulnerable to attacks as each device acts as a relay. Any tampering with the routing information can be compromise the whole network. An attacker can introduce rogue information with in routing information or replay old logged or stored information. The aim is to protect any information or behavior that can update or cause a change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. For completeness, timeliness and ordering are added to the list of desirable security properties that can eliminate or reduce the threat of attacks against routing protocols. Techniques that can be used to guarantee these properties are described in Table1

Table 1: Properties of secured routing

Properties	**Techniques**
Timeliness	Time stamping, Slotted Time
Ordering	Sequence Numbering
Authenticity	Password, Certificate
Authorization	Credential
Integrity	Digest, Digital Signature
Confidentiality	Encryption
Non-Repudiation	Chaining of Digital Signature

Biometric Devices: Biometrics refers to automatic identification of a person based on his or her physiological behavioral characteristics [7]. It states that biometrics provides a better solution for increased security requirements of the information society than the traditional identification methods such as passwords. Some of the biometric technologies being used today include, facial imaging both optical and infrared). Hand and finger geometry, eye-based methods (iris and retina), signature, voice, vein geometry, keystroke, and finger-and palm-print imaging [7] .

Digital watermarks: Digital watermarks are electronic signatures placed on content to identify its legitimate owner and the user, as well as any licensing agreements to use the content. The literature explains [8] the usage of digital watermarks to prevent piracy and assist jurisdictional issues raised from the ownership disputes of intellectual property on the Internet. In another research paper, [6] explains two digital watermarking models for resolving rightful-ownership-issues, one of which explains how the digital watermark can be used for identifying the legitimate user of the content.

Access Tokens: Access tokens are small electronic devices, combined with suitable hardware and software can be effectively used for secure authentication of users. Some of the access tokens such as SecurelID Token from [9] generates unpredictable, one-time-only access codes that automatically change every 60 seconds. Such systems can be linked to information systems to effectively authenticate users.

Code Signing: Code signing enables organizations to securely deliver files over the Internet [10]. Code signing is often established on the basis of trust, aided by sophisticated cryptographic technologies. If the file has been changed in any way after it has been digitally signed, the signature will be corrupted and software will alert the user that the code has been altered and is not trustworthy. Most of the Web browsers are capable of working with Code Signing software.

Digital certificates: a digital security certificate is a text file that contains certain information that is used by the secure socket layer protocol to establish a secure connection. a security certificates contain information about who it belongs to, who it was issued by a unique serial number or other unique identification, validity and an encrypted finger prints that can used to verify the contents of certificates. Certification authorities such as verisign issue security certificates.

Smart cards: these are credit card like devices with an embedded electronic chip, which can store account and identification information for uses such as electronic banking and security identification. Possible applications of smart cards are virtually limitless. A smart card in conjunction with a card reader and suitable software can store almost any type of information, and there are several smart card applications in the market today. One of the major obstacles to the widespread adoption of smart cards is often referred to as incompatibility among smart card applications, and the lack of standards.

III. EXISTING CRYPTOGRAPHY TECHNIQUES

A message, made unintelligible by altering it according to a certain procedure can be made intelligible again by applying a reverse procedure. The scrambling of messages can be done at the level of whole words or at the level of individual letters and numbers. Encryption systems that work at the word level are technically known as codes; those that work at the letter level are known as ciphers. Typically there are 5 techniques, which are used in conjunction with one another, for scrambling a message. They include [7]:

- **Substitution** – The first step in the substitution process is to create a substitution table, designating the replacement character for each character that may appear in a message. Each letter of the message is systematically encoded to match its corresponding substitution number or letter. To decode the message, the reverse process is utilized.
- **Blocking** – Encryption systems often divide a message into blocks of characters that can be independently manipulated. The resulting blocks are stacked vertically and then realigned so that each block contains the same number of characters. The ciphertext is then created by linking the blocks together in a horizontal stack and transmitting in sequence. The receiver groups the ciphertext into vertical columns and then reads the message.
- **Permutation** – Permutation is one of the most important encryption techniques utilized today. Also known as transposition, it involves moving characters around according to specific rules; the characters keep their identity but not their position. This technique is the opposite of substitution where letters keep their position and change their identity.
- **Expansion** – A simple way to obscure a message is to stretch it according to a fixed recipe. In actual cryptographic practice, the recipe is quite elaborate although the technique is easily ciphered.
- **Compaction** – Reducing the length of a message or reducing its number of blocks is another way of rendering a message unreadable. The components that are removed are done so at set intervals and are transmitted separately. The combination of removed letters and the rule for removing them makes up the key for deciphering the message.

IV. PROPOSED PACKET ENCRYPTION ALGORITHM

At the initial stage, the data packet will be transmitted from source to destination over transmission media using efficient cryptographic algorithm to encrypt the entire packet. Cryptography is the process used to make a meaningful message appear meaningless. An algorithm is a set of rules or procedures used to scramble, or encrypt the plaintext to produce Ciphertext. The algorithm applies a key to text [5]. Encryption is the procedure that guarantees secrecy of the data exchanged. Any encryption algorithm depends on some key, and keys are normally generated during authentication phase, so the two phases are strictly connected [2]. In the proposed architecture, an extended flavor of link level encryption will be used to encrypt the entire data packet. The packet encryption algorithm at the originating site encrypts the entire packet including the packet header and provides it a new header. This readable new header also includes a

dynamic key-id. The key-id controls the behavior of encryption and decryption mechanism. It specifies the information as the encryption algorithm, the encryption block size, the error checking code and lifetime of the key.

ENCRYPTION ALGORITHM

Step 1: Activate and Initialize the Packet P_i

Step 2: Generate a Random Key K_R by analyzing number of 1s in Packet.

(a) Develop a routine to count bits in the Data Packet

(b) Set N := Count(P_i) // Count Number of 1's in the Data Packet.

(c) Set K_R :=N // Store N in Random Number K_R

Step 3: Apply XOR (Exclusive-OR) Operation

(a) Set E_K := $P_i \oplus K_R$

(b) The Encrypted Packet E_K is generated using XOR Operation.

(c) Set PE_K :=E_K // Utilize E_K as Encrypted Packet

Step 4: Packet equipped for Transmission

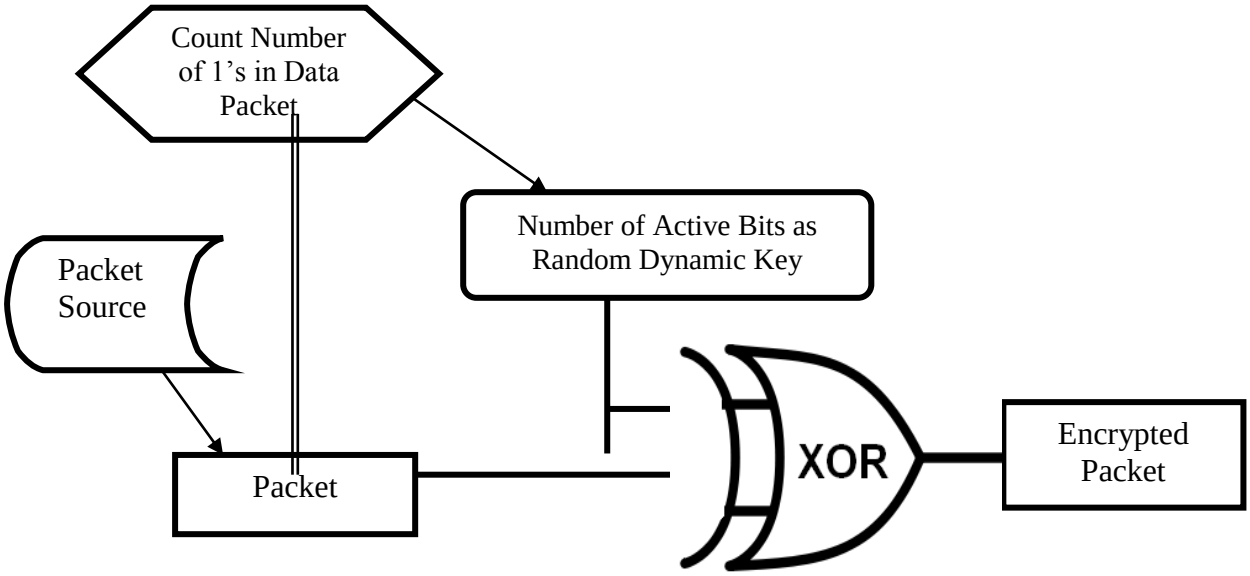


Figure 2: Algorithm description

EXAMPLE OF ENCRYPTION ROUTINE

Suppose we have a Data Packet with following Bit Stream –

10101010 10001000 00001010 11101010

The packet is represented as a 4 Byte or 32 Bits Data Packet.

Number of 1's in each byte are 4, 2, 2, 5

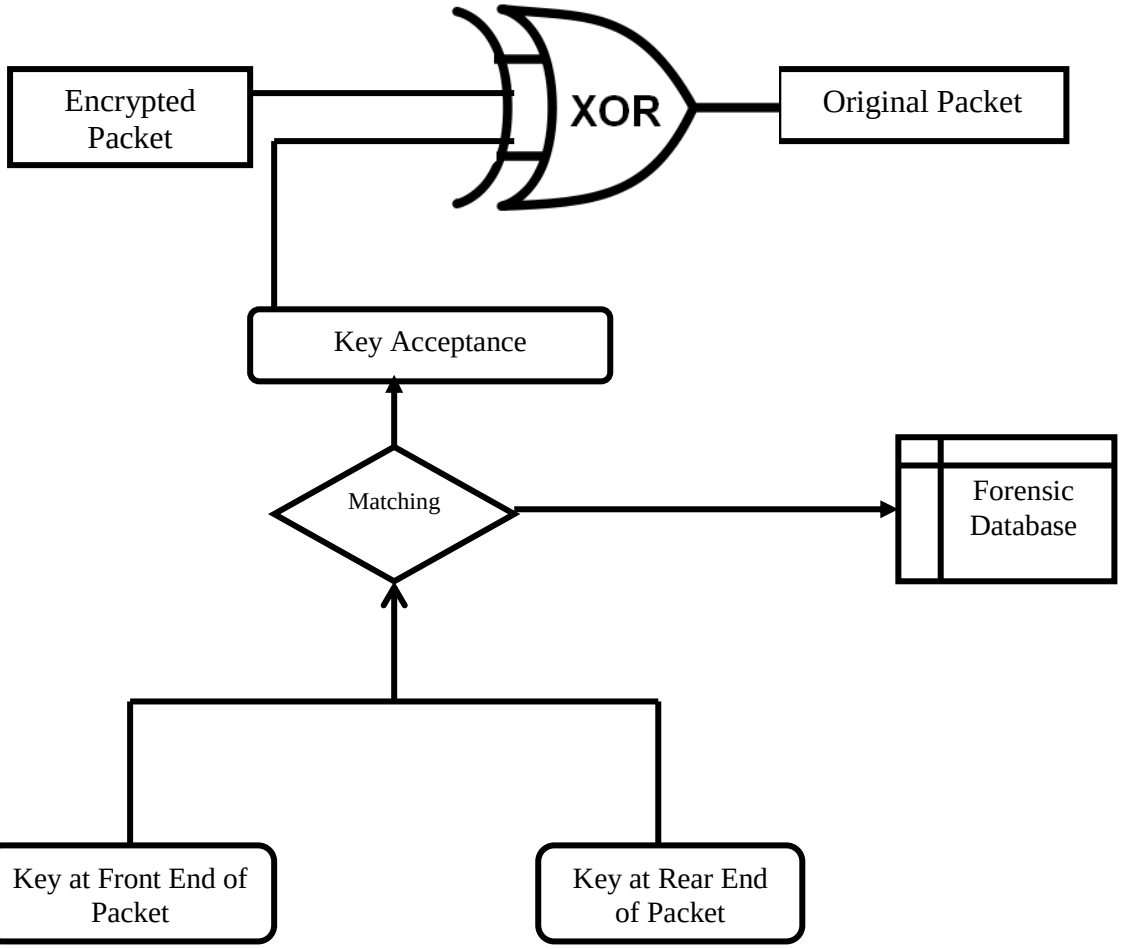
Binary Equivalent of 4, 2, 2, 5 are 0100, 0010, 0010, 0101

BITWISE XOR OPERATION FOR ENCRYPTION OF PACKET

Actual Packet	10101010	10001000	00001010	11101010
Key	00000100	00000010	00000010	00000101
Encrypted Packet	*10101110*	*10001010*	*00001000*	*11101111*

DECRYPTION AND INTERCEPT DETECTION ALGORITHM

A decryption algorithm at the destination site will check the entire encrypted packet. The received packet will be of specific format and structure in which key is given. By analyzing the structure of encrypted packet, the location of key will be accessed and the packet can be decrypted. In case of interceptions at the transmission line, the details of such attempts will be stored in the web based databases so that interception points and sources can be identified. In case, there is an interception and packet is not matched after decrypting the Ciphertext C_p, a record will be inserted in the forensic database. The pattern/behavior of intercepts will be analyzed using a forensic analyzer. In case of successful decryption and transmission of packet, an acknowledgement will be transmitted to the web based database where the source site can verify the delivery of message.



ALGORITHM

Step 1: Receive the Encrypted Packet PE_K
Step 2: Check the Front PF_i and Rear End PR_i of Packet
if ($PF_i = PR_i$)
Accept PFi
Set $K_R := PF_i$
Else
goto Step 5
Step 3: Generate the Binary Equivalent of K_R
$PB_i = Binary(K_R)$
Step 4: Perform XOR Operation
if ($PB_i = PE_K$)
Decryption Successful
Accept the Packet
else
goto step 5
Step 5: Insert the Record of Corrupt Packet in Forensic Database

EXAMPLE OF DECRYPTION ROUTINE

Key	00000100	00000010	00000010	00000101
Encrypted Packet	10101110	10001010	00001000	11101111
Actual Packet	10101010	10001000	00001010	11101010

V. CONCLUSION

Networks are facing challenges from increasing interceptions and cracking attempts through various sources. There is need to secure the data packets roaming around the network from multiple interceptions using efficient cryptographic

algorithms. The packet encryption algorithm explained in the paper is an efficient algorithm based on Exclusive-OR operation which is a unique method. Using this method, encryption and decryption can be performed effectively with unique cryptographic technique without any complexity. Moreover, the forensic database will keep record of every invalid or unacceptable decrypted packet.

REFERENCES

[1] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 2002.

[2] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia

[3] A.Kush,Sima,Vishal ,"Securing Manet against Hacking" , intl conf on applied and communication tech, **Elsevier Publ,** pp 121-126., 2014

[4] Security, Encryption, Acceleration, http://www.networkintercept.com

[5] Youlu Zheng, Shakil Akhtar, Networks for Computer Scientists and Engineers, Oxford University Press, 2009

[6] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004

[7] *R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance Evaluation of Fingerprint Verification Systems", IEEE Trans. Pattern Anal. Mach. Intell,2006*

[8] http://www.papermasters.com/encryption-techniques.html Last Visited Sept. 8, 2013

[9] *Kaufman, C., Perlman, R., & Speciner, M. "Network Security: Private Communication in a Public World", Englewood Cliffs (NJ): Prentice Hall, 2004.*

[10] *Dharma Prakash Agrwal ,Qing-An Zeng, "Introduction to Wireless and Mobile Systems",(2007)*

[11] S. Taneja, A. Kush and C. Jinshong Hwang , "Key Exchange for Securing Adhoc Networks", 3rd International Conference on Computer Engineering and Technology (ICCET 2011), Session 15 - Communication and Broadband Networking, Kuala Lumpur, Malaysia, pp. 933-940, June 17-19, 2011, ISBN: 9780791859735 (Print) ,

