International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 08, August 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

NODE VERIFICATION IN WIRELESS NETWORK

Pratik Singh[1], Dr. Bhawna Mallick[2]

[1,2]Department of Computer Science and Engineering,
Galgotias College of Engineering & Technology, Greater Noida(India)

ABSTRACT

Proof of user identity on network is just like challenge for current scenario. Node verification is the vital procedure for wireless communication. We proposed a verification technique that use hash code for verification and also proposed 2D cryptography technique to maintain data integrity and confidentiality during transmission.

Keywords: Verification, Cryptography, And Hash Code, Security Attacks, Security Analysis.

I. INTRODUCTION

Security is an encapsulated concept includes authenticity of user, integrity and confidentiality of data during transmission. In wireless communication there are more threats for breach the security due to the openness of wireless network and no boundary limitations. It is free for access and anyone can easily access the network or steel the identity of other to access the network in the absence of proper security mechanisms. So verification of node is a primary step regarding to verify the authenticity of a user. There are a number of verification techniques exist some of our as digital signature, certification , mapping of pilot symbols, third party verification in this a trusted third party verify the nodes who participate in communication. Verification is required in every field of networks such as sensor network (WSN), mobile ad-hoc networks (MANETs), vehicular ad-hoc networks (VANETs).

In this paper, we proposed a node verification technique in which receiver verify the sender before receiving the data. If receiver verify then message accept otherwise reject the message. It exists on physical layer based on hash code. A unique hash code generated from message and transmits with message to verify the sender. We also consider other security threats which break the confidentiality and integrity of data during transmission such as impersonate attack, Substitution attack, replay attack, jamming attack etc. some data is very confidential such as military data, research data, transaction data which security is a major issue during transmission. For this we proposed a 2D cryptography technique, encrypt data before transmission at sender node and decrypt at receiver node. We also analyze our proposed techniques against various security threats. The paper is organized as follows. In section II, we discuss about the system model, followed by the discussion on the security issues and analysis in section III. Simulation and results are discussed in section IV, simulation and result. Finally, in Section V, we conclude the paper, and references are given at the end of the paper

International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 08, August 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

II. CONSIDER SCENARIO

We consider a scenario fig.1 in wireless network there is a sender, a receiver and a passive attacker, and a active attacker. Sender sends a message via insecure wireless network. Passive attacker only performs detection/monitoring or traffic analysis of data and ruptures the confidentiality of data but

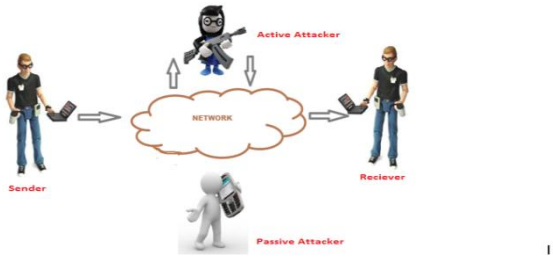

Fig.1.Proposed Scenario

active attacker not only split the confidentiality but also ruptures the integrity of data through inject her own data that is called impersonate attack and if replace data then it is called substitution attack.

III. PROPOSED HASH CODE GENERATION ALGORITHM 1

In this section, we propose a simple and efficient hash generation algorithm. Our proposed algorithm works as a hash function. The hash function takes the input message of any size but return the output in a fixed size hexadecimal code. In this algorithm, and hash code is generated by the use of message and shared key.

$$\text{Hash code} = G(M,K) \qquad (1)$$

Generated hash code is impracticable to find another message that yields the same hash code. If there is any change in either key or message then generated hash is also
Differ.

Algorithm 1: Hash Code Generation

Initialize
Enter message (M)
Enter shared key (K)
begin
Convert message into ASCII
Perform xor operation on each ASCII value
For i = 1:length(M)
X(i) = bitxor (M(i), K)
Add all values after bitxor to get a single no.
len=length(X);
for i=1:len;
N=X(i)+N;
end

```
Maximize no.
while (N<65535)
   N=M*2;
end
Convert decimal no. into hexadecimal
Hash_Code = dec2hex(N)
end
```

IV. PROPOSED 2D POLYNOMIAL CRYPTOSYSTEM

After generating the hash code from message now message is encrypted by proposed 2D polynomial cryptography algorithm 2 and yields cipher text data C. In this we consider a 2D polynomial equation and based on that perform symmetric encryption.

$$C = \text{encrypt}(M, \text{key}) \quad (3)$$

After performing encryption on message, cipher text is concatenate with the hash code and yields data D which will be modulate

$$D = C + \text{hash code} \quad (4)$$

$$T = \text{modulate}(D) \quad (5)$$

Now Signal T transmitted to receiver by a reference signal but there is reference signal equal to the modulated signal. So receiver receives

$$Y = h.T + w \quad . \quad (6)$$

Where h is channel estimation and w is noise. Receiver recovers T from received signal Y and demodulates it. After get combine data receiver separate the hash code and encrypted message from the combine data and decrypt the encrypted message (C) as equation (7), the procedure of equation (7) described in algorithm 3.

$$M = \text{decrypt}(C, \text{key}) \quad (7)$$

Thus regenerate the hash code from equation (8) by use the shared key and message

$$\text{Re\_hash code} = G(M, K) \quad (8)$$

This regenerated hash code compared with the received hash code if both the hash codes are same then the sender node is verifying, otherwise discard the sender node.

Algorithm 2: 2-D Polynomial Encryption

Intialize
Enter message (M)
Enter key for encryption (key)
begin
Convert m into ascii values
M=ASCII(M)
: for i=1:len(M)
enc(i)=power((key+M(i)),2);
end
convert ascii code into character
cipher_text = char(enc)
C=cipher_text
end

Algorithm 3: 2-D Polynomial Decryption

Initialize
Enter key for decryption (key)
begin
Construct a 2D polynomial
p= key^2+2*key*m-enc
Find roots(r_1,r_2) of polynomial (p)
If (r_1>0)
Decrypt=r_1
Else
Decrypt=r_2
End
Plain_text=char (Decrypt)
end

V. SIMULATION AND RESULT

For simulation we use MATLAB R2010A. QPSK modulation technique is used to modulate the data at transmission bit rate is 1000000. Channel (h) is assumed to be ideal and the length of messages is varying according to our requirements and assumed that shared key k is known to both transmitter and receiver.
Now we focus on the effect of noise on acceptance rate.

Fig. 3 shows that acceptance rate is directly proportional to the SNR (Signal to Noise Ratio) as the SNR increases acceptance rate also increases.

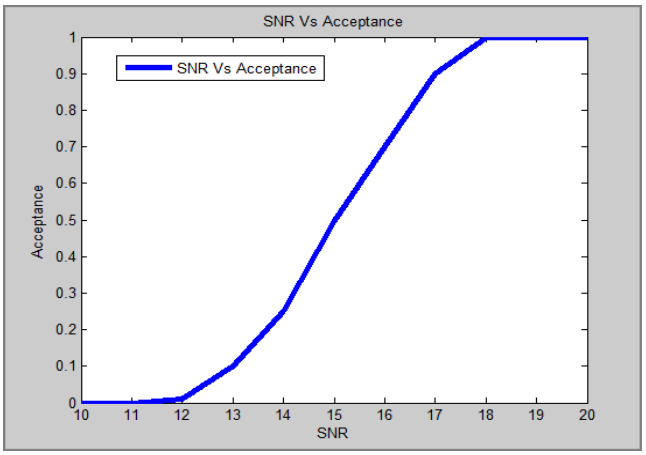

Fig.3 Accepted Messages at Various SNR

We also focus the subject of message length on the acceptance of message at receiver. Fig. 4 shows the effect of msg. length on acceptance rate, there is acceptance rate is inversely proportional to the msg. length, as length of messages increases acceptance rate decreases.

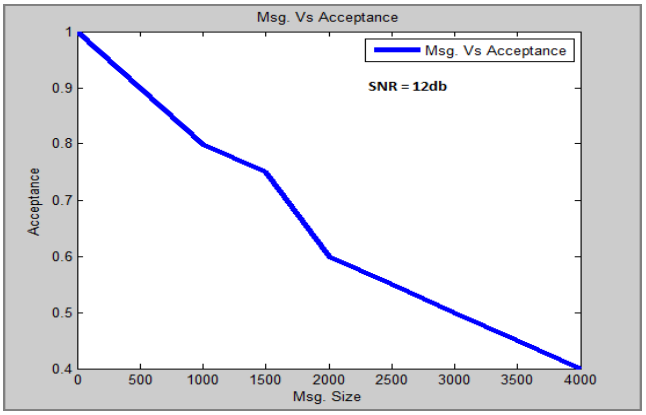

Fig.4 Acceptance at Various Message Sizes

In table 1, show that for various keys and messages, proposed algorithm of hash code generation generate different hash codes, if there are hash code generate for same message with, in both cases we get two different hash codes and vice versa of these cases at serial no. 3, 4and 8 that we use same key for two different messages then also generated two different hash codes, which show that our proposed hash code generation algorithm satisfy all the conditions of hash code discuss above.

TABLE 1

S. NO.	MESSAGE	KEY	HASH CODE
1	node verification	23	EDC0
2	node verification	67	C280
3	engineering and technology	56	84A0
4	computer science	56	A120
5	Hash code depend on key and message	45	F168
6	Alice is a better sender	55	DA78
7	Bob is a attacker	89	8788
8	Bob is a attacker	56	A2A0
9	wireless sensor network	123	8A98
10	Hash code depend on key and message	45	F168

VI. SECURITY ANALYSIS

In this section we perform the security analysis of proposed techniques against various security threats

6.1 Passive Attacks: A passive attacker only observed the data during transmission and extract the important details , lose the confidentiality of data but in our proposed scheme encryption is perform on data before it transmitted . So there is no hazard to lose the confidentiality of data.

6.2 Substitution Attacks: In this, active attacker replace the message and insert her its own message with a previous captured hash code, so receiver accept this message but in proposed verification scheme hash code is generated from message and key and hash code generating function is very sensitive, if a single bit of message change then the generated hash code must be change.

6.3 Impersonation Attacks*:* In this active attacker may be more fury and try to generate her own hash code for their messages and send her own generated hash code with the messages to Bob and hope he will be accepted it. In proposed scheme the hash code generation function depends on message as well as shared key, so it is challenging to detect the shared key.

VII. CONCLUSION

In this research paper, we have proposed a hash code based sender node verification scheme in wireless and hash code is directly generate from message and shared key, then perform encryption on message before transmission, so the confidentiality of data maintain during transmission where hash code is used to verify the sender node, Simulation of proposed hash code generation algorithm illustrate that our algorithm satisfy all the properties of a hash code and each time generate a unique hash code. We also focus on the noise and message size impact on verification rate and analyzed the proposed scheme against various security threats which demonstrate the toughness of our node verification scheme.

REFERENCES

[1] Horn G., Preneel B., "Authentication and Payment in Future Mobile Systems." ComputerSecurity - ESORICS'98, Lecture Notes in Computer Science, 1485, 1998, pp. 277-293.

[2] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in Proc. of the fourth ACM conf. on Wireless network security, Hamburg, Germany, Jun. 2011.

[3] L. Lamport, "Password authentication with insecure communication," Commun. of the ACM, vol. 24, no. 11, pp. 770–772, 1981.

[4] Paul L. Yu, John S. Baras ,"Physical-Layer Authentication ",IEEE transactions on information forensics and security, vol. 3, no. 1, march 2008.

[5] B. Danev, H. Luecken, S. Cˇ apkun, and K. Defrawy, "Attacks on Physical layer Identification," in WiSec '10: Proceedings of the 3th ACM Conference on Wireless Network Security. ACM, 2010, pp. 89–98.

[6] Dan Shan, Kai Zeng, Weidong Xiang, Paul Richardson, and Yan Dong "PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks",IEEE Journal on selected areas in communications, vol. 31, no. 9, september 2013.

[7] Marco Baldi, Marco Bianchi, Nicola Maturo, Franco Chiaraluce"A Physical Layer Secured Key Distribution Technique for IEEE 802.11g Wireless Networks" IEEE wireless communications letters, vol. 2, no. 2, april 2013.

[8] Kapil M., Borle Biao Chen ,Wenliang Du "A Physical Layer Authentication Scheme For Countering Primary User Emulation Attack" IEEE 2013 .

[9] Xianru Du∗, Dan Shan∗, Kai Zeng,"Physical Layer Challenge-Response Authentication in Wireless Networks with Relay",IEEE INFOCOM 2014 - IEEE Conference on Computer Communications 2014.

[10] Liang Zhou, Dan Wu, Baoyu Zheng, Mohsen Guizani" Joint Physical-Application Layer Security for Wireless Multimedia Delivery" IEEE Communications Magazine , march 2014