International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Avoiding Brute Force attack in MANET using Honey Encryption

Vinayak P P[1], Nahala M A[2]

[1]Final year M. Tech Cyber Security, KMP College of Engineering, Odakkali, Aluva Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, KMP College of Engineering, Odakkali, Aluva Kerala, India

Abstract: ***Mobile adhoc network includes wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure. This MANET is vulnerable to different types of attacks due to the certain features of network. Lot of attacks are there in MANET .Brute forcing is one of the attack that can create problem in communication in a MANET network. Mainly focusing on single hoc MANET Honey encryption can prevent such attacks during the normal encrypted data transmission. This is new type of encryption in which when an attacker tries to brute force by different keys different decrypted data will be got, thus the brute forcer will be confused totally about the actual content. A new type of randomized message encoding scheme called a distribution-transforming encoder (DTE).***

Keywords: MANET, One-Time Pad, Honey Encryption, DTE, attack.

1. Introduction

This paper gives an idea of implementing a new encryption schema that will prevent a change of brute forcing in simple MANET single hock network. MANET network is having two types of structure one is single hop and multi-hope .A lot of security vulnerabilities are there in MANET , this is due to the peer to peer architecture, highly dynamic network topology and nodes openness to physical capture. There are a lot of attacks normally seen in MANET, and here we are focusing on a type of attack called brute forcing. Brute forcing is a process to decode the data which is in encrypted form by providing different keys.

Normal encryption has lot of drawback as comparing the new one, if an attacker tries a key to decrypt the data in a normal encryption error symbols will be displays and thus the attacker will tries to brute force and create problem. Normally in MANET a lot of attacks has been detected but a change of brute forcing is also there. Real world system replies for encryption in very low entropy .The existing password based encryption(PBE) was developed for increasing the strength of the password with the help of salting, in cryptography salt means it is a random data that is used as an additional input to a one way function that will hashes a password. Main peculiarity of the salt is for each password a new random salt is generated, then the salt and password are concatenated and processed with a hash function and so. Hash functions are represented by H and with respect to password it is h(p) and with respect to the salt it is h(p,s).The basic PBE will slow the attack by the multiple users and so. More over to avoid the recovery of the encrypts messages by trying different passwords or keys we developed the new encryption schema called Honey Encryption." Honey Encryption is a security tool that makes it difficult for an attacker who is carrying out a brute force attack to know if he has correctly guessed a password or an encrypted key.

2. Related Work

Different attacks where taken into concern in Manet network and it solution to avoid for the type of attack was discovered in earlier .The attacks in Manet can be classified into mainly tow types one is passive and active attacks.

Table 1: Types of attacks

Blackhole Attack	Active Attack
Denial of service	Active Attack
Rushing Attack	Active Attack
Sinkhole Attack	Active Attack
Sybil Attack	Active Attack
Traffic Analysis	Passive Attack
Wormhole Attack	Active Attack

The data that is transmitted from a sender node to the receiver node in Manet network will be in encrypted form and if an attacker id present in between and if he tries to decrypt the data by trying different keys has change to get the data to be decrypted ie Via brute force attack. This chance of attacker is not taken into the consideration .To avoid the chance of this attack our proposed encryption scheme is useful. To brute force the key of password attacker can use sophisticated tools such as John the Ripper and so, this tools can easily crack the hashes when the underlining passwords are weak.

2.1 Development of Password-Based Encryption

This encryption schema is also vulnerable to brute force attack. PBE consist of two main function such as enc and dec function .To encrypt a message such as L , the working is like first L is encrypted with a password P and the corresponding cipher text C is produces ie L=dec(C). If the password or key which is used to decrypt the encrypted message id wrong an error message will be produced. Mostly the error message will be of symbols mostly seen symbol is "| ".The security of the PBE is fully depended on the attacker's ability to guessing ability of the password. By using the hacking tools

this schema can be crashed. To avoid this problems of this brute force attack we proposed the new and secure encryption schema called Honey encryption.

3. Proposed System

Honey encryption provides an efficient security against brute force attacks for some kind of messages .Here the working is like the honey encryption provides a cipher text C that decrypts under any key or password that is provided by the attacker and it will be plausible looking message .The fake key or password will get a fake message when trying to decrypt the data that looks like valid to an attacker as it is the actual message .the internal structure of the honey encryption includes a specialized encoding schema and a normal encryption schema .

This example will describe the working of the procedure of honey encryption ie Anu's password manager database is encrypted with HE and decrypts under an incorrect master password *P* * to yield a list of fake passwords or accounts. An attacker who tries these passwords online will fail to impersonate anu's.

3.1 Approach to honey encryption:

There are two types of approaches for honey encryption, they are
1) The onetime pad
2) Distribution transforming encoding

3.1.1 The onetime pad:

A chipper mechanism with a security against an unbound attack technique is called as one time pad. Here the message L is expressed in chipper as K bit string($L \in \{01\}^k$).Then by the XOR bitwise operation the message and key are combined C=L⊕X, and the key has been masked .Given C every possible K bit message L is an equally possible plaintext because a key X exits such as C=L'⊕X'.In this way Shannon security is achieved for this technique.

Still we cannot say that one time pad is not a pure honey encryption technique because of some reasons because the key must have the same length as of the message L and because of that it provides strong entropy ie strong password or key that is used for the encryption. As per the honey encryption mechanism the system must work in weak password also, another reason is most of the keys are failed to produce the plausible plain text and instead corresponds to a random string.

3.1.2Distribution Transforming Encoding

The main idea behind pure honey encryption is the DTE (distributed transforming encoding), here Honey encryption models the space of plaintext via DTE. Let the probability distribution over the message space be p over the message L. user L for encryption with a probability p.

The distribution transforming encodes message L as a K bit seed S$\in \{0,1\}^k$, and decodes the message by inverse DTE decode (S) =L.DTE is a good model of the message distribution. The internal structure of the HE includes DTE encryption and DTE decryption .The two algorithm describes the net functioning of the Honey encryption.

Honey Encryption Algorithm (a)
HEnc(X, L)
S← $ encode(L)
R← $ {0, 1}n
S' ←H(R, X)
C ←S'⊕S

Honey Decryption Algorithm (b)
HDec(X, (R, C))
S'←H(R, X)
S ←C ⊕S'
L←decode(S)
return L

H is a cryptographic hash function, X is a key, L is a message, S is a seed, R is a random string, C is a cipher text, and ← denotes uniform random assignment. When we apply HE to the message L, first we encode the message L to S and the encrypt S by a key X using suitable symmetric encryption algorithm .The above algorithms describes the steps clearly, Honey encryption provides high message recovery security.

The functioning can be described by an example encrypting soft drink flavours, Here it includes three flavours such as grape, orange, pineapple etc. this encrypted items will have a two bit string such as {00,01,10,11} etc.

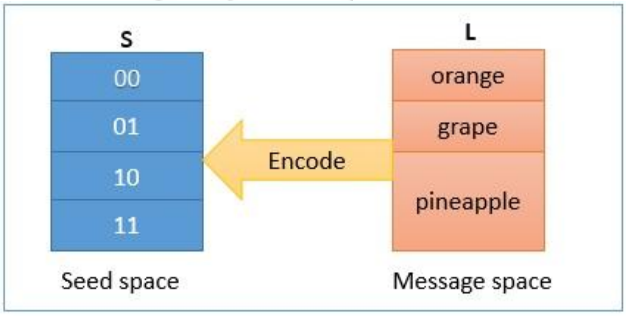

Figure 1: The message "orange" (with pm = 1/4) maps to 00, "grape" (with pm = 1/4) maps to 01, and "pineapple" (with pm = 1/2) maps to {10, 11}. pm is a probability distribution over the message space.

Honey encryption can be described but this example let's assume Ram want to encrypt his favourite soft drink flavour L= Grape that is to be send to r=Roopa under a secret key =0000 that is shared with Roopa. Ram construct a flavour soft drink DTE that maps the message L into the into the space of 2bit strings {00, 01, 10, 11}.The working is like via DTE the encoded orange will have the value 00 and encoded pineapple will have the value 10 or 11 which is randomly chosen .The message encoded by ram that is grape is having the value 01. Ram selects a random string R and computes S'=H(R,X) and assume that S'=(R,0000)=11 and then the Ram computes C=11⊕01=10 and it is forwarded to Roopa.

Roopa decrypts C by the key that has been shared by the Ram that is key X=0000. So S'=H(R,0000)=11, and

S=C⊕S'=10⊕11=01 and the ecode(01)=Grape and the message is successfully recovered by the Roopa. Suppose an attacker C tries to decrypt it .He doesn't know the key that is used so he assumes key such that of 1432, H=(R, 1432)=00 and then S''=C⊕S'=10, and by decoding it he will get decode(10)=pineapple. Thus the attacker is fooled by this new type of encryption and so.

4. Conclusion

Here it is clear that by using this type of encryption it is clear that an attacker can be fooled easily by this new technique called honey encryption that is the brute force attacker cannot gain the correct message when they try to decrypt it with their keys. This technique can be used in MANET network and so.

References:

[1] Honey Encryption Encryption beyond the Brute-Force 1540-7993/14/$31.00 © 2014 IEEE Copublished by the IEEE Computer and Reliability Societies July/August 2014
[2] M.L. Mazurek et al., "Measuring Password Guessability for an Entire University," Proc. 2013 ACM Conf. Computer and Communications Security (CCS 13), 2013, pp. 173–186.
[3] I.H. Witten, R.M. Neal, and J.C. Cleary, "Arithmetic Coding for Data Compression," Comm. ACM, vol. 30, no. 6, 2007, pp. 520–530
[4] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Tech. J., vol. 28, no. 4, 1949, pp. 656–715.

Author Profile

Vinayak.pp received the B.Tech degree in Information Technology from University Of Calicut in 2011 and currently pursuing final year M. Tech degree in Computer Science and Engineering with specialization in Cyber Security from KMP College of Engineering, Perumbavoor.

Nahala M.A received B.Tech in Computer Science & Engineering from Mahatma Gandhi University Kottayam in 2010 and M.Tech in Computer Science & Engineering from Mahatma Gandhi University Kottayam in 2014 and currently working as Assistant Professor in KMP College of Engineering Perumbavoor in Computer Science and Engineering Department.