ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Secured Hello Handshake Authentication (SHHA) in MANET

[I]N.Sivabalasubramanian, [II]T.Parameswaran, [III]R.Ramkumar
[I,III]PG Student, [II]Assistant Professor, CSE,
Anna University Regional Centre, Coimbatore,Tamil Nadu, India,
E-mail : siva.bala1989@gmail.com, tparameshse@gmail.com, kkrram88@gmail.com

Abstract
Mobile Ad-hoc network (MANET) is a wireless network between the mobile nodes without any centralized administration and infrastructure. Due to the node mobility, the network topology may change rapidly and unpredictably over time. Additionally, some nodes cannot communicate directly with each other because nodes in a MANET normally have limited transmission ranges. Hence, routing paths in MANETs potentially contain multiple hops, and each node in MANETs has the responsibility to act as a router. So the protocols and algorithms designed for MANET should be distributed in order to accommodate a dynamic topology and an infrastructure less architecture. In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation. The aforementioned characteristics of MANET lead to security breaches in MANET. Securing a MANET is very challenging because MANETs is vulnerable to various kinds of security attacks like worm hole, black hole, rushing attack etc. From the study about attacks in MANET, most of the attacks are launch during route discovery such as Gray Hole, Black Hole and Flooding and selfish the dangerous one. So each node should authenticate the neighbor node during route discovery with the help of Cryptography. SHHA is proposed to each node validates the trustworthiness of neighbor node during neighbor node discovery. SHHA provides one hop authentication using the symmetric key encryption without any centralized node. Symmetric key is periodically generated distribute manner in each legitimate node. Each node ID is encrypted using symmetric key. The encryption of node ID increases the strength of security in MANET. This technique confines the malicious node to disrupt the communication.

Keywords
MANET, SHHA, Symmetric key, Session ID, Authentication.

I. Introduction

MANET is used in highly security sensitive applications such as battlefield communications, emergency relief circumstances and law enforcement. But MANET is highly susceptible to many attacks due to the possessions of MANET such as infrastructure less, the absence of trusted centralized nodes, and mobility. A main challenge of MANET is security of legitimate nodes from malicious node by detecting and separating the malicious nodes from the legitimate nodes. The basic requirements for a secured networking are secure protocols which ensure the confidentiality, availability, authenticity, integrity of network [3]. SHHA accomplish the basic requirements for secure protocol through the cryptography.

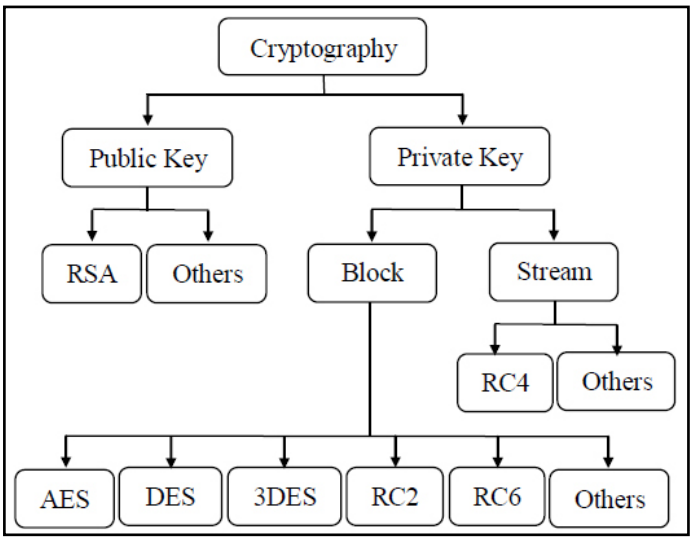

Fig 1: Classification of Cryptography

Cryptography plays a crucial and powerful role in the field of network security. Cryptography is the art of secret writing. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. Decryption is the process of converting encrypted text to normal text in the readable form. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric key encryption, only one key is used. Symmetric key encryption divided into to stream and block cipher. In Asymmetric keys, two keys are used: private and public keys. Public key is used in sender side for encryption and private key is used in receiver side for decryption (E.g. RSA and Digital Signatures). However, asymmetric key encryption is computationally intensive and is not very efficient for mobile devices because asymmetric key is based on mathematical functions, [1]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [2].

Secured Hello Handshake Authentication (SHHA) technique is proposed to authenticate an each neighbor node during the neighbor node discovery. This technique uses the symmetric key and Session ID for neighbor node authentication. Symmetric key is periodically generated in each legitimate node. Session ID is a unique identifier of each hello message broadcasting in each legitimate node.

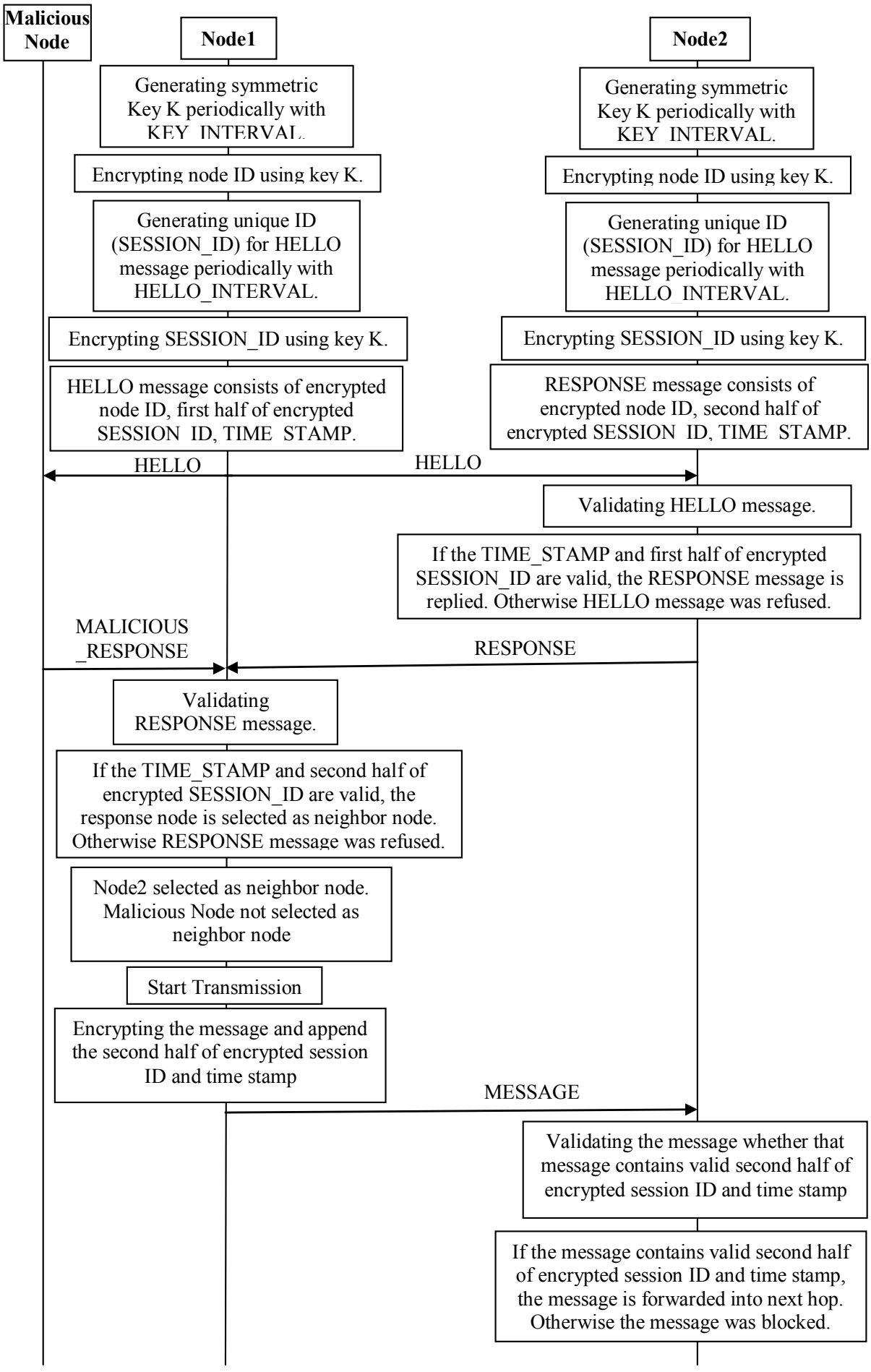

Fig. 2. Architecture of SHHA

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Symmetric key encryption is used for encrypting Node ID, Session ID and messages. This technique authenticates the neighbor node through the Hello and Response message Hello message consists of encrypted Node ID, first half of the encrypted Session ID and Time stamp. Response message consists of encrypted Node ID, second half of the encrypted Session ID and Time stamp. Each node having the Session ID so we can use this for validates the two nodes of each link. Neighbor nodes validate the Hello message by check the first half of the Session ID and Time stamp. If first half of the Session ID and Time stamp are valid, the Hello message is considered as valid and forward response to source of the link. Otherwise the Hello message is considered as invalid and refused. Source of the link validates the Response message by check the second half of the encrypted Session ID and Time Stamp. If second half of encrypted Session ID and Time stamp is valid, responded node select as neighbor. Otherwise responded node is not select as neighbor node.

SHHA provides security to MANET in three levels. First level of security is provided through encrypting the Session ID and data. Second level of security is provided through authentication during the neighbor node discovery. Third level of security is provided through authentication during the transmission. SHHA prevents the MANET from the most of the attacks because this technique implemented in neighbor node discovery. This technique provides high security with efficient.

2. Secured Hello Handshake Authentication (SHHA)

(i) Symmetric key and Session ID generation:

Encryption key is a very significant component of cryptography. In MANET, using and managing keys for security is a crucial task due its energy constrained operations, limited physical security, variable capacity links and dynamic topology. Centralized key distribution violates the important characteristics of MANET (infrastructure less network). So SHHA proposed a new distributed key generation technique named as Distributed Time Based Symmetric Key Generation Scheme (DTBKGS) for Symmetric key generation. DTBKG periodically generates the symmetric key in each node using current time. Time is divided into date, month, year, hour and etc. Initially, the set of keys are loaded using random numbers. Distributed Time Based Symmetric Key Generation algorithm is shown in below algorithm 1. Session ID is unique identifier of each neighbor node discovery. Session ID is periodically generated in each node. SHHA proposed a new scheme for Session ID generation named as Distributed Time Based Session ID Generation Scheme (DTBSIDGS). But the interval of Session ID generation is very lower than the time interval of symmetric key generation. Distributed Time Based Session ID Generation Scheme shown in Algorithm 2.

Algorithm 1:

Algorithm DTBSKG ()
Begin
1: Initialize the Key array with N elements;
2: Fetch current time;
3: Separatethe week day (WEEK_DAY) part, date part and time part;
4: Separate the date (DD), month (MM), year (YYYY) from date part;
5: Separate the hour (HH) and minute (MIN) from time part;
6: Sum_of_Date=DD+MM+YYYY;
7: Sum_of_Time=HH+MIN;
8: If (Time is Morning) Then
9: SESS=2;
10: Else
11: SESS=3;
12: End If
13:Index1=(Sum_of_Date^(SESS* WEEK_DAY)) MOD N
14: Index2= (Sum_of_Time ^ (SESS * WEEK_DAY)) MOD N
15: Symmetric_ Key=Key [Index1] XOR Key [Index2]
End

Algorithm 2:

Algorithm DTBSIDGS ()
Begin
1: Fetch current time;
2: Separate the week day (WEEK_DAY) part, date part and time part;
3: Separate the date (DD), month (MM), year (YYYY) from date part;
4: Separate the hour (HH), minute (MIN) and second (SEC) from time part;
5: Sum_of_Date=DD+MM+YYYY;
6: Sum_of_Time=HH+MIN;
7: If (Time is Morning) Then
8: SESS=2;
9: Else
10: SESS=3;
11: End If
12: Index1= (Sum_of_Date ^ (SESS * WEEK_DAY * SEC));
14: Index2 = (Sum_of_Time ^ (SESS * WEEK_DAY *SEC));
15: Session_ID=Var1 * Var2;
End

(ii) Encryption:

Symmetric key encryption is also called as secret key encryption or private key encryption. In symmetric key encryption, only one key is used to encrypt and decrypt data. Strength and performance of Symmetric key encryption depends on the size of key used. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [2]. Blowfish has better performance than other common encryption algorithms used, followed by RC6 [4, 5, 6, 7].

Each node ID is encrypted by Blowfish encryption algorithm using the symmetric key. This encryption of node ID is performed distribute manner during symmetric key generation. The encryption of node ID will help to hide the node identities from malicious node and prevents identity impersonation. It increases the security level of MANET. SHHA scheme encrypts the Session ID using blowfish encryption algorithm in each node before the hello message broadcasting. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits (14 bytes). The algorithm was developed to encrypt 64-bits of plaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwise exclusive-or to minimize the time required to encrypt and decrypt data. A conscious attempt was made in designing the algorithm to keep the operations simple and easy to code while not compromising security.

Encryption Algorithm:

Algorithm Encryption()
Begin
1: Divide x into two 32-bit halves: xL, xR.
2: For i = 1 to 16:
3: Do
4: xL = xL XOR Pi
5: xR = F(xL) XOR xR
6: Swap xL and xR
7: End For
8: xR = xR XOR P17
9: xL = xL XOR P18.
10: CipherText= xL + xR
End

Now that the P-array and S-box values have been established, plaintext can now be encrypted. For encryption, the 64-bit plaintext is separated into a left and right half each consisting of 32-bits. The encryption routine consists of a 16 round Feistel network. In the first round, an exclusive-or operation is performed between the left 32-bits (LE-0) and the 32-bit P1 of the P-array. This value becomes the next 32-bit right value (RE-1) and this value is also inserted into the F function. The F function takes the 32-bit input and separates it into 4 bytes (8-bits each). These four values are then used for table lookup in their respective S-Boxes. Unlike DES which uses more bits to map to S-boxes, Blowfish only uses four 8-bit values for mapping to the S-box values. A less complex mapping was used because the S-boxes are generated from the key values and are not static like DES.

(iii) Authentication:

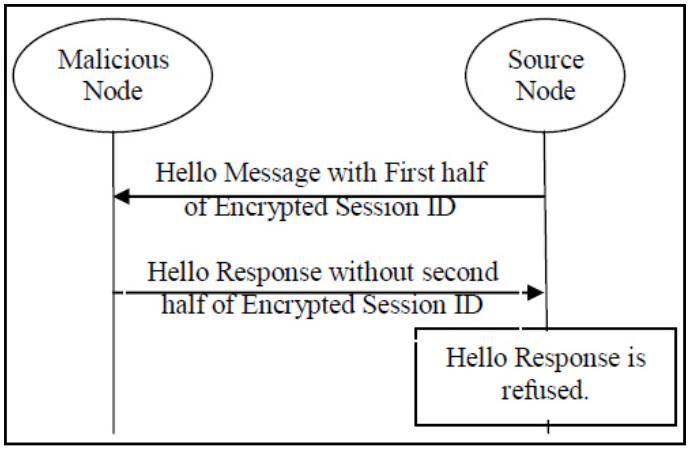

Fig 3: Malicious Node Detection and Prevention

Authentication is a process of validating the nodes whether legitimate or attacker node. Authentication performed through the encrypted session ID during neighbor node discovery. Encrypted session ID is periodically generated in each node. Encrypted session ID is partitioned into Left and right encrypted session ID. Left encrypted session ID and time are appending to the hello message. The Hello message format is shown in figure 4.

HELLO MESSAGE	SESSION ID	TIME STAMP

Fig 4: Hello message format

Hello message is broadcasted into neighbor node Neighbor node validates the hello message contains valid left half of encrypted session ID and time. If the hello message contains valid left half of the session ID and time, the hello message considered as a valid hello messages and the source node considered as a legitimate node. Otherwise the source node of hello message is considered as a malicious node and refuses the hello message. Malicious node detection and prevention is shown in Figure 3.

RESPONSE MESSAGE	SESSION ID	TIME STAMP

Fig 5: Response message format

The neighbor nodes are responses for the valid hello message. The second half of the encrypted session ID and time append to the response message. The response message is shown in Figure 5. Source node of hello message receives and validates the received hello response contains valid second half of the encrypted session ID. If the hello response contains valid second half of the encrypted session ID and time, the node considered as a legitimate node and select as a neighbor node. Otherwise the nodes are not select as a neighbor node. Legitimate node detection is shown in Figure 6.

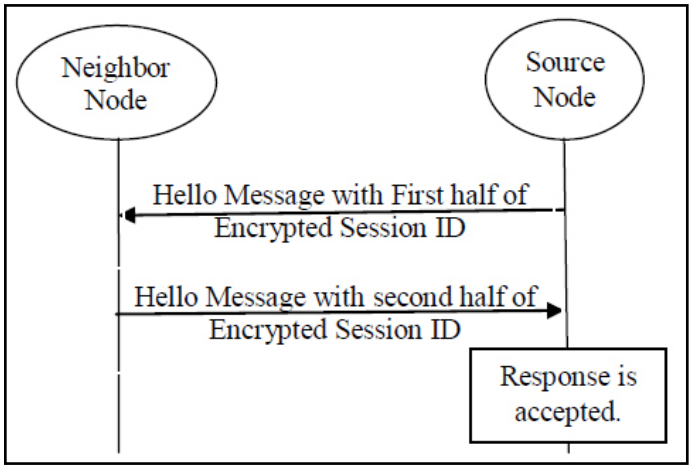

Fig 6: Legitimate Node Detection and Transmission

Source Node Authentication Algorithm:
Algorithm Source_Node_Authentication ()
Begin
1: Generating Symmetric Key (K);
2: Generating Session ID (S_ID);
3: ENC_S_ID=E (S_ID,K);
3: ENC_ID=E (ID,K);
4: Divide ENC_S_ID into three halves L_ENC_S_ID and R_ENC_S_ID;
6: Broadcast HELLO_MSG;
7: Receive hello response HELLO_RESP;
8: Separating the hello response (HELLO_RESP) second half of the encrypted Session ID (RECEIVED_R_ENC_S_ID) and time stamp REC_TIME_STAMP;
9: If (RECEIVED_R_ENC_S_ID == R_ENC_S_ID and REC_TIME_STAMP is valid) Then
10: Select as a Neighbor Node;
11: Else
12: Response is refused;
13: End If
End

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Neighbor Node Authentication Algorithm:
Algorithm Neighbor_Node_Authentication ()
Begin
1: Generating Symmetric Key (K);
2: Generating Session ID (S_ID);
3: ENC_S_ID=E (S_ID,K);
3: ENC_ID=E (ID,K);
4: Divide ENC_S_ID into two halves L_ENC_S_ID and R_ ENC_S_ID;
5: Receive hello message (REC_HELLO_MSG);
6: Separating REC_HELLO_MSG into hello message (HELLO_ MSG) ,first half of the encrypted session ID (RECEIVED_L_ ENC_S_ID) and Time Stamp (REC_TIME_STAMP);
7: If (RECEIVED_L_ENC_S_ID == L_ENC_S_ID and REC_ TIME_STAMP is valid) Then
8: HELLO_RESP= HELLO_RESP + R_ENC_S_ID+TIME_ STAMP;
9: Reply HELLO_RESP
10: Else
11: Refuse HELLO_MSG
12: End If
End

(iv) Transmission:

After the neighbor node discovery, the data is encrypted using symmetric key in the source node. First half of the encrypted session ID is append to the encrypted data. The data is transmitted from source to destination through the hops. Encrypted node identities only used during the transmission. It prevents the MANET from impersonation attack. In each hop, the first half of encrypted session ID is verified. If the first half of encrypted session ID is available and valid, the encrypted message is transmitted to next hop. Otherwise the transmission will be blocked. The encrypted data is decrypted in the destination node.

ID_S	ID_D	MESSAGE	SESSION_ID

Fig 7: Data packet format

III. Performance Evaluation

In this section, we provide experimental evaluation of the Secured Hello Handshake Authentication, which exhibit consistency with our analytical results. Both prove the superior performance of Secured Hello Handshake Authentication in providing authentication with low cost of overhead. We compare Secured Hello Handshake Authentication with typical MANET.

1. Network Models

We use two different network models, random way point model and group mobility model with the random way point model as the default setting, and we also compare the performance of Secured Hello Handshake Authentication in the group mobility model. In the group mobility model, we set the movement range of each group to 150 m with 10 groups and to 200 m with five groups.

2. Parameters

The tests were carried out on NS-2.29 simulator using 802.11 as the MAC protocol with a standard wireless transmission range of 250 m and UDP/CBR traffic with a packet size of 512 bytes. The test field in our experiment was set to a 1000 m X 1000 m area with 100 nodes moving at a speed of 2 m/s, unless otherwise specified. The density was set to 50, 100, 150, and 200 nodes per square meters. The duration of each simulation was set to 100 s unless otherwise indicated. The number of pairs of S-D communication nodes was set to 10 and S-D pairs are randomly generated. S sends a packet to D at an interval of 2 s. We use the following metrics to evaluation the routing performance in terms of effectiveness on anonymity protection and efficiency:
Power: This is measured by power taken for communication between the source and destination.
Delivery rate: This is measured by the fraction of packets that are successfully delivered to a destination. It shows the robustness of routing algorithms to adapt to mobile network environment.

3. Delivery Rate and Power :

In this experiment, we evaluated the performance of the SHHA. Delivery rate of the MANET with SHHA was compared with delivery rate of the MANET without SHHA. Delivery rate of the MANET was evaluated with respect to the number of malicious node. Figure 8 shows the delivery rate of SHHA model and without SHHA model. It can be seen that the delivery rate of MANET with SHHA higher than the delivery rate of MANET without SHHA. Even the number of malicious node increases, SHHA provides stabilized delivery rate of the MANET. Power is an important constraint in MANET. So we considered the power as a factor in performance evaluation. Power consumption is slightly increased when using SHHA in MANET. But SHHA provides good security for MANET from malicious nodes.

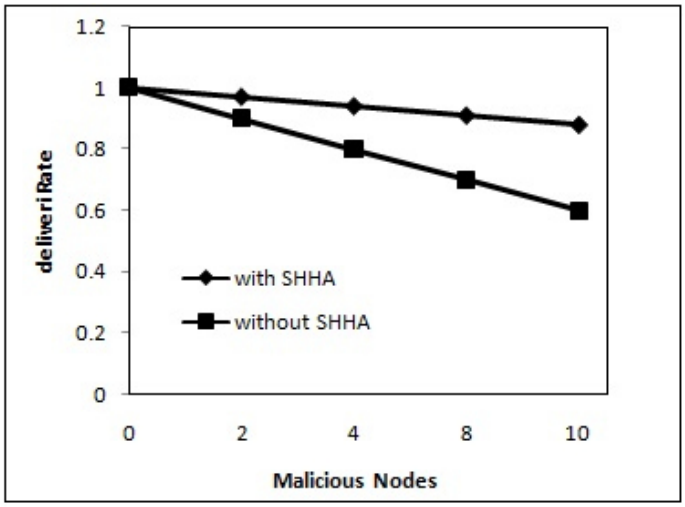

Fig 8: Transmission Delivery Rate

IV. Conclusions

This paper presented the SHHA technique, which in neighbor node authentication in suspicious MANET. SHHA provides the three levels of security to the MANET. It generates the symmetric key in distribute manner without any centralized node and key distribution. It does not share any key between the nodes. It transmits only encrypted data by using highly dynamic keys. So the attackers can not crack the keys or encryption algorithm. SHHA provides high security to the MANET from most of the all attacks. In MANET, security is a challenging task because power consumption of cryptographic algorithm. To improve the proposed work, power consumption of cryptographic algorithm will be reduced by introducing energy efficient cryptographic algorithms.

References

[1] *P. Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N, " The Third IEEE Workshop on Wireless LANs - September 27-28, 2001- Newton, Massachusetts.*

[2] *Hardjono, "Security in Wireless LANS and MANS, " Artech House Publishers 2005.*

[3] *Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), Vol-1, Issue 5, June 2012*

[4] *Gurjeevan Singh, Ashwani Kr. Singla, K.S. Sandha, "Superiority of Blowfish Algorithm in Wireless Networks", International Journal of Computer Applications, Vol 44, No11, April 2012*

[5] *M. Anand Kumar, Dr.S.Karthikeyan, "Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms", I. J. Computer Network and Information Security, March 2012, pp 22-28*

[6] *Pratap Chnadra Mandal, " Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, No 9, September 2012, pp 196-201*

[7] *Ali Ahmad Milad, Hjh Zaiton Muda, "Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack)", Journal of Computer Science, 2012, pp 1191-1197*

[8] *S. Abbas, M. Merabti, D. Llewellyn-Jones and K. Kifayat, "Lightweight Sybil Attack Detection in MANETs," IEEE SYSTEMS JOURNAL, vol. 7, no. 2, Jun 2013*

[9] *M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," Int. J. Netw. Security, vol. 9, no.1 pp. 22–33, Jul 2009.*

[10] *S. Capkun, J. P. Hubaux, and L. Buttyan, "Mobility helps peer-to-peer security," IEEE Trans. Mobile Comput., vol. 5, no. 1, pp. 43–51, Jan. 2006.*

[11] *Y. Chen, J. Yang, W. Trappe and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Trans.Veh. Technol., vol. 59, no. 5, pp. 2418–2434, Jun. 2010.*

[12] *K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.*

[13] *V. Frias-Martinez, S. J. Stolfo, and A. D. Keromytis, "BARTER: Behavior profile exchange for behavior-based admission and access control in MANETs," presented at the Proc. 5th Int. Conf. Information Systems Security, Kolkata, India, 2009, pp. 193–207.*

[14] *K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.*

[15] *N. B. Margolin and B. N. Levine, "Quantifying resistance to the Sybil attack," in Financial Cryptography and Data Security. Berlin, Germany: Springer, 2008.*