An Efficient and Secure Data Transmission of Common Randomness Routing in Adhoc Wireless Network

Duvvada Shreya Sri[1], R.V.L.S.N Sastry [2]
Final M.Tech. Student[1], Associate Professor [2]
[1, 2] M.Tech Computer Science and Engineering, Sri Venkateswara College of Engineering and Technology, Etcherla, Srikakulam (District), Andhra Pradesh

Abstract:

Now a day's automatic key establishment of any two devices in the network is placed an important role and generation of key is used for public key based algorithm. By using public key based algorithm we can automatically generated secret key any two devices in the network. So that by performing this process we can randomly generate secret key. In the ad hoc networks another concepts is routing from source node to destination node. The generation of routing process can be done by randomly and performing this process we can improve the efficiency in the routing. In this paper we are implementing random routing of secure data transmission protocol for generating routing and provide privacy of transferred message. By implementing this protocol we can provide random routing process for transferring message. Before transferring message the server will randomly generate routing for source node to destination node. After that the source node will send data to destination node. Before transferring message or data the source node will encrypt and send the cipher format data to destination node. The destination node will retrieve cipher format data and perform the decryption process. After completion of decryption process the destination node will get original message. By implementing those concepts we can improve the efficiency for generating routing and also provide security of transferring message.

Keywords: *Security, Secret Key Establishment, Common Randomness, Dynamic Source Routing.*

I. INTRODUCTION

The wireless network is a collection of hundreds and thousands of low cost and low power mobile nodes connected by links.[1]. The Centralized Administration Mechanism does not contains MANET operation. In the Routing Network properties each node act as a "router" to forward the traffic to other specified node in the network. In the MANET Wireless network is a self-configuring network of mobile routers connected by links with no access point. In the Wireless Network Mechanism each mobile devices are free to move and organize themselves arbitrarily. In the MANET Networks Each Nodes share the wireless medium and the topology of the network. The advancements in wireless communication and the miniaturization of computers have led to a new concept called the mobile ad hoc network (MANET), where two or more mobile nodes can form a temporary network without need of any existing network infrastructure.

The Proposed Network helps to improve routing process and also provide more security of transferred data. By implementing the proposed system each time we can generate new path for transferring data from source node to destination node. So that each time will choose new routing path for transferring data. In the process of implementation we can also provide security of transferred data. To provide security of transferred data we can use cryptography technique. By implementing the cryptography technique we can easily perform the encryption and decryption process. In the encryption process we can generate only one key for performing encryption process and decryption process. In this process we can use same key for encryption and decryption process. Here we cannot share the secret key, so that we cannot chance to get the key. After completion of encryption process we can easily perform the encryption process with data containing repeatedly. In the existing cryptography technique are caterogarized into two types. One of the Symmetric key and another one is asymmetric cryptography. By implementing symmetric key cryptography technique we can use only one for encryption and decryption process. In the asymmetric key cryptography technique we can use private key encryption process and public key is decryption process. By implementing those technique if chance know any key we can easily get original data. So that by overcome those problems we can proposed this process.

The advantage of wireless communication to share data anywhere through ad hoc network (MANET). In the wireless network more than one mobile nodes can form a temporary network without need of any existing network infrastructure. [2] By implementing proposed system will helps to improve the throughput and to reduce the packet loss and packet delay. We

propose a random routing mechanism to prevent attackers from tracing back to locate source location hop by hop under the constrained offset angles and constrained probability. [3] The key establishment, the problem is traditionally generate the randomness stage and agreement stage. In the public-key infrastructure or on symmetric encryption process we are using single key for encryption and decryption process. In the wireless network we can perform route discovery phase of an ad-hoc network.in the wireless Communication networks are unpredictable and highly dynamic. To implement the randomness routing is easily accessible networking metadata so that we can avoid traffic loads, dropped- packet rates or packet delays. It can be easily available to the devices that took part in the routing process, but it is usually unavailable to those devices that were not part on the route. It discuss about the routing protocol, where the routing information could be used for establishing secret common randomness between any two devices in a mobile ad-hoc network.

II. RELATED WORK

Jon W. Wallace (2010) considered the non-coherent reaches of secret key simultaneousness with open exchange over free indistinctly passed on Rayleigh obscuring remote channels, where neither the sender nor the recipients have section to quick channel state information (CSI). We show two results. At high banner to-bustle extent (SNR), the secret key point of confinement is constrained in SNR, paying little personality to the amount of receiving wires at each terminal. Ashish Khisti and Suhasi (2012) creator giving arrangement on meddler watches a source grouping related with the honest to goodness terminals. Mystery key limit is set up when the sources grouping of the meddler and the channel of the spy are debased renditions of the relating source and channels at the true blue recipient.

At the point when an open discourse channel is accessible propose creating separate mystery keys from sources and channels and build up its optimality in some exceptional cases. a mystery key assertion procedure that saddles vulnerabilities from both sources and channels. Second, for a structure with a single receiving wire at both the true blue additionally, the spy terminals and a subjective number of transmit receiving wires, the puzzle key cut off fulfilling input dissemination is discrete, with a predetermined number of mass core interests. Numerically we watch that at low SNR, the utmost achieving spread has two mass centers with one of them at the origin. Record Terms Discrete data scattering, information theoretic security, Karsh Kuhn Tucker (KKT) condition, non-coherent capacity, Rayleigh obscuring channels, and secret key comprehension.

Krishna Kumar et al (2015) proposed Secret key understanding between two or numerous gadgets in a system is typically needy upon an open key framework. Be that as it may, in the situations when no such framework exists, or when the existent framework is not dependable, clients are left with generally couple of strategies for setting up secure correspondence. Our lower bound rate expression includes selecting a working point that adjusts the commitment of source and channel prevarications. Its optimality is built up for the instance of conversely corrupted parallel channels. KERMAN depends on the course disclosure period of an impromptu system utilizing the Dynamic Source Routing convention. The calculation is assessed for different system parameters, and two unique levels of many-sided quality, in an OPNET impromptu system test system. Our outcomes demonstrate that, in a brief span, a huge number of mystery irregular bits can be produced organize wide, between various matches in a system of fifty clients.

III.PROPOSED SYSTEM

In the proposed system we are implementing random routing of secure data transmission protocol. By implementing this protocol we can generate secret key, generate randomness routing, encryption and decryption of transferring message. In the generation of secret key the source node and destination node will generate secret key.

A. Nodes initiation process

In this module each client will send request to server for communication process. After completion communication process the server will generate client id and port number. After generating those values the server send to each and every client. Before performing the communication the server will generate points (X_i, Yi) for each node and send to the each node in a wireless sensor network. The implementation of secret key is as follows.

B. Secret Key Generation Process

1. In the Key Generation process the source node and destination node will choose P and G values are the prime numbers.

2. After completion of prime numbers the source node will choose private key (a). By using those values the source node will calculate public key by using following formula.

$$\text{Public key} = G^{a} \bmod p$$

3. The completion of public key source node will send public key to destination node.

4. The destination node will retrieve public key and choose the private key (b). By taking those values the

destination node will calculate the public key by using following formula..

Destination public key= G^b mod Pl

5. After completion of public key generation the destination node will send the public key to source node.

6. The source node will retrieve public key and generate shared key by using following formula.

Shared key= destination public key ^{a} mod P

6. The destination node will retrieve source node public key and generate shared key by using following formula.

Shared key= source node pubic key ^{b} mod P

After that source node and destination node will get same type of secret key. The completion of secret key generation process the source node will enter transferred message and perform the encryption process. After completion of encryption process the data will transferring to server. The server will generate routing from source node to destination node. The generation of routing can be done by randomly and implementation of routing is as follows.

C. Route Discovery Process

In the route discovery process the source node will send request to server and the server will generate random routing by using following process.

1. The server will retrieve all client distance points individually.

2. Take those points and the server will find out difference between source nodes to other nodes by using the following formula.

diff= sqrt(X2- X1+Y2-Y1)

3. After calculating difference the server will generate random path and calculating distance of all paths by adding difference.

4. Take those values of all routers and find out minimum distance of path. Take that path and send the data through that path.

Before finding the shortest path source node will enter transferred message and perform the encryption process. The implementation process of encryption is as follows.

D. Encryption:

P=plain Text

1. Take the plain text data and add the randomized characters in between the plain text. For every 3 characters we can add one duplicate character in the plain text.

2. Get the ASCII codes for the each characters from the plain text and convert into binary format.

3. After completion of Binary format we can perform the complement.

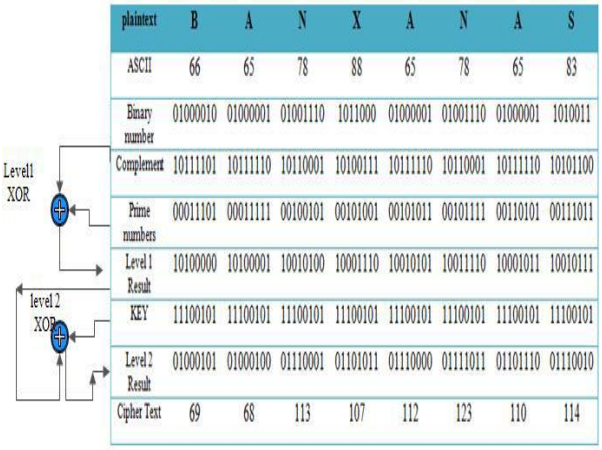
4. Select series of prime numbers based on length of plain text data and convert those values into Binary format.

5. Take the binary values of prime number and plain text data perform the first level Exclusive OR (XOR).

6. After completion of xor operation Select any Randomized number (key) key th prime number from the prime numbers table.

7. Take that key value and perform the Second level of XOR operation between result of step5 and Randomized prime number.

8. Take those result values of step 7 and Convert into decimal values. Now you will get the cipher text.



plaintext	B	A	N	X	A	N	A	S
ASCII	66	65	78	88	65	78	65	83
Binary number	01000010	01000001	01001110	1011000	01000001	01001110	01000001	1010011
Complement	10111101	10111110	10110001	10100111	10111110	10110001	10111110	10101100
Prime numbers	00011101	00011111	00100101	00101001	00101011	00101111	00110101	00111011
Level 1 Result	10100000	10100001	10010100	10001110	10010101	10011110	10001011	10010111
KEY	11100101	11100101	11100101	11100101	11100101	11100101	11100101	11100101
Level 2 Result	01000101	01000100	01110001	01101011	01110000	01111011	01101110	01110010
Cipher Text	69	68	113	107	112	123	110	114

The completion of encryption process the source node will take those cipher format data and send to destination node through path. The destination node will retrieve cipher format data and perform the decryption process. The implementation process of decryption is as follows.

E. Decryption

1. The receiver will take the cipher format and Convert into Binary format. Take Key from prime numbers table and convert it into binary format.

2. After converting perform the first level of Exclusive OR (XOR) operation between cipher texts and Key.

3. The receiver will take the series of prime numbers and convert it into the binary format (the series must be same in both encryption side and decryption side).

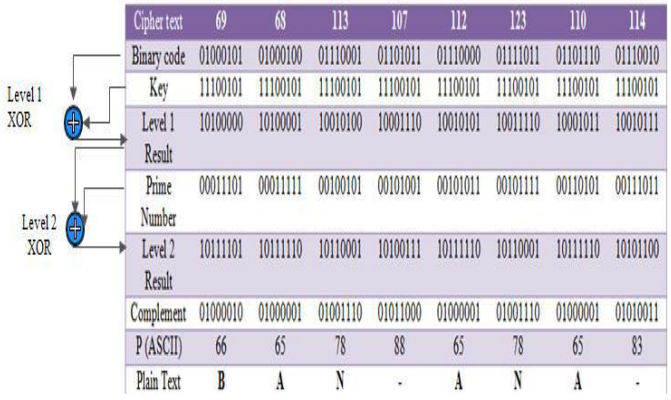
4. After completion of first level xor operation do second level of XOR operation between result of step2 and series of prime numbers.

5. Take second level xor operation result and perform the complement.

6. Take complement data and Convert into decimal format.

7. After that take those decimal values and convert into characters. Take those result data and Remove added character from the result data.

8. After removing we will get original plain format data.



Cipher text	69	68	113	107	112	123	110	114
Binary code	01000101	01000100	01110001	01101011	01110000	01111011	01101110	01110010
Key	11100101	11100101	11100101	11100101	11100101	11100101	11100101	11100101
Level 1 Result	10100000	10100001	10010100	10001110	10010101	10011110	10001011	10010111
Prime Number	00011101	00011111	00100101	00101001	00101011	00101111	00110101	00111011
Level 2 Result	10111101	10111110	10110001	10100111	10111110	10110001	10111110	10101100
Complement	01000010	01000001	01001110	01011000	01000001	01001110	01000001	01010011
P (ASCII)	66	65	78	88	65	78	65	83
Plain Text	B	A	N	-	A	N	A	-

III.CONCLUSIONS

In this paper we are proposed a secret randomness routing process for transferring data from source node to destination node. Before transferring data the source node and destination nodes generating common secret key. By using secret key the source node will encrypt transferred message and send to destination node. The source node will enter transferred message and also take the secret key. By using secret key the source node will encrypt transferred message and convert into cipher format. Take those cipher format data and send to destination node through server. The server will retrieve cipher format and also get source node, destination node ids. After that the server will generate shortest route randomly. After generating shortest route the server will send cipher format data to destination node through shortest path. The destination node will retrieve cipher format data and perform the decryption process. By perform the decryption process the destination node will get original plain format data. By implementing those concepts we can improve efficiency in routing process and also provide more security of transferred data.

REFERENCES

[1] V.Joseph and G. de Veciana, "Nova: Qoe-driven optimization of dash based video delivery in networks," arXiv preprint arXiv:1307.7210, 2013.

[2] Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[3] W.Diffie and M. E. Hellman, "New directions in cryptography," Information Theory, IEEE Transaction on vol. 22, no.6, pp.644-654,1976.

[4] Khisti, A and G. Wornell, 2012. "Secret-key generation using correlated sources and channels," Information Theory, IEEE Transactions on, 58(2): 652-670.

[5] Mukesh Singhal, 2012. "Key Management Protocols for Wireless Networks"international journal.

[6] Park, S.K and K.W. Miller, 2009. "Random number generators: good ones are hard to find," Communications of the ACM, 31(10): 1192-1201.

[7] Renner and S. Wolf, 2005. "Simple and Tight Bounds for Information Reconciliation and Privacy Amplification",pp: 199-216.

[8] Shuangqing Wei† S and Jing Deng, 2015. "KERMAN: A key establishment algorithm based on harvesting randomness in Manets" 14,April

[9] Ren, K and Q. Wang, 2011. "Characteristics in wireless communications," Wireless Communications, IEEE, 18(4): 6-12.

[10] Sunar, B., 2009. "True random number generators for cryptography," in Cryptographic Engineering. Springer, pp: 55-73.

[11] Ye, C and P. Narayan, 2012. "Secret key and private key constructions for simple multi terminal source models," Information Theory, IEEE Transactions on, 58(2): 639-651.

[12] Wang, Q., H. Su and K. Kim, 2011. "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in infocom, Proceedings IEEE, pp: 1422-1430.

[13] Ueli M. Maurer, 2011. "Secret key Agreement By Public discussion from common Information" IEEE Transaction, March.