Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 5583-5588*

Research Article

A Privacy Preserving and Efficient Randomness Routing in Adhoc Wireless Network

G.Asha Jyothi[a], Dr. Sri Ram Chandra Polisetty[b], *K. Suryakala[c]

[a,b,c*] Faculty of Engineering, Computer Science and Engineering, Godavari Institute of Engineering and Technology (A), Rajahmundry, Andhra Pradesh, INDIA

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

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

1. Introduction

An ad hoc network is a collection of hundreds mobiles and low power mobile nodes connected by wireless links.[1] The nodes in mobile adhoc network was not have a centralized mechanism. In the wireless network each node act as router to forward data to other node in the network. By transferring data through MANET is a self-configuring network to connect by wireless links with no access point. In the adhoc network each mobile device is autonomous. By implementing adhoc network mobile devices are free to move and organize themselves. Each Node in the MANET share the wireless medium and the topology

of the network dynamically The advancements in wireless communication and the mobile ad hoc network where two or more mobile nodes can form a temporary network without need of any existing network infrastructure. The implementation of proposed work helps to improve the privacy of transferred data and to reduce the packet loss and packet delay. The research of secret common randomness proposes an efficient routing strategy and also provide secure of data. . By implementing this approach will increase the reliability of data transmission. The multipath routing protocols are used to reduce the routing overhead, delay and to increase the data rate. By providing routing protocols to discover the paths every time when it is required to communicate with other nodes.

By implementing proposed system to provide more efficiency in the routing process and also improve the secret key generation between communication nodes. The proposed work helps to improve the throughput of transferred data and also reduce the data loss in the network. By implementing this approach we can also increases the packet delivery ratio and also increase the reliability of data transmission. To implementing the multipath routing protocols are used to create different routing each time and to overcome the route discovery overhead. In this paper we are proposed different routing mechanism and also provide better cryptography technique for security of data. So that by implementing cryptography to provide more security and also overcome the loss the data in the adhoc network. Before transferring data from source node to destination node the server will generate random shortest routing protocol for communicating each other.

Mobile adhoc network is used establishes secret common randomness between two or multiple devices in a network. By implementing this routing process it provide secure communication nodes. [3] In this paper we can also implemented one more concepts is key establishment, that overcome the problem of symmetric and also each user will generate its own secret key. So that the communicate nodes only knows those key and other nodes not known other keys. By provide this process we can reduce single operation for entire nodes. After that

completion of the key generation process the server node will generate randomness routing generation stage and an information agreement stage. After completion of information agreement the server will transfer data to destination node. The destination will retrieve cipher formatted through specified path and perform the decryption process. By implementing route discovery phase of an ad-hoc network employing the Dynamic Source Routing Protocol. It is lightweight and requires relatively little communication overhead. The Communication random ness routing networks is highly dynamic and not a predictable. The randomness is usually not easily accessible networking metadata such that to overcome traffic loads, packet delays or dropped- packet rates. By implementing this routing process it can be easily available to the devices that took part in the routing process. 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.

2. Related Work

P. Sri Ram Chandra et all proposed a new symmetric stream cipher cryptography algorithm with a title Ultramodern Encryption Standard (UES) for secure data transmission which uses prolic series number for generating set of keys, binary and gray code operations for encryption and decryption processes. If an intruder intercepts the message, it is difficult to decipher the message because of multilevel cipher rounds used in this algorithm. They have analyzed the strength of this algorithm over differential cryptanalysis. This algorithm unfailingly follows the Strict Plaintext Avalanche Criterion (SPAC) and Strict Key Avalanche Criterion (SKAC).

P. Sri Ram Chandra et all have proposed a new symmetric block cipher named Modular Encryption Algorithm with an acronym MEA which uses tri-modular matrix for its key generation, a set of operations on a matrix, Permutations and Substitutions for its encryption and decryption. As part of operations required in MEA authors have proposed M-Box, the functionality is described in their work. The multilevel cipher rounds used in this algorithm can enhance the security such that even an intruder intercepts the message, it could be difficult to decipher the message. The strength of this algorithm has been analyzed over differential cryptanalysis. This algorithm undoubtedly follows the Strict Plaintext Avalanche Criterion (SPAC) and Strict Key Avalanche Criterion (SKAC) - the Shannon‘s property of ―Confusion‖ and ―Diffusion.

Krishna Kumar et al 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. In this paper, we talk about KERMAN, a secret common haphazardness foundation calculation for impromptu systems, which works by reaping haphazardness straightforwardly from the organize directing metadata, along these lines accomplishing both unadulterated irregularity era and (certainly) mystery key assertion. 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.

Ashish Khisti and Suhasi 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. 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.

Jon W. Wallace 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. 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.

3. Proposed System

In this paper we are proposed an efficient random routing for secure transmission data in the adhoc network. By implementing random new routing protocol we can generate secret key, generate randomness routing, encryption and decryption of transferring message. In the generation of secret key the source and destination nodes are communicating each other and generate unique secret key for data encryption and decryption process. After generating secret key the sender node will enter transferred message and perform the encryption process. The completion of encryption process the sender will send data to destination node. Before sending data to destination node the server will generate random routing from source node to destination node. Take that route for transferring data and the destination node will retrieve cipher format data. The destination node will take cipher format data and perform the reverse process of encryption will get original plain format data. By implementing those techniques we can improve more efficiency on routing and also provide more security of transferring message. The implementation process of all those techniques is as follows.

Initiation Process of Nodes:

In the node initiation process each node will send request to server for generating communication process. The communication process can be done by sending ip address and port number of server. After sending request the server will accept and generate communication between nodes. Before performing the communication process the server will generate points (Xi, Yi) for each node and send those details to each node in a wireless sensor network. After completion of sending values the source and destination nodes are generate secret key. The implementation of secret key is as follows.

Generation of Secret Key:

In this module the generation of secret key can be done between the communicated nodes in the network. Before the transferring data to source node the destination node will choose the communicate node. After choosing communication nodes will perform implementation process of secret key. The implementation of secret key is as follows.

The communicate node of source and destination nodes will choose two prime numbers P and G.

After choosing the source node will enter our private key (a) and calculate the public key using following formula.

Public key = G a mod p

The sender node will take the public key and send to destination node.

The sended public key will retrieve by the destination and the destination node will choose his/her own private key (b). After completion of this process the destination node will calculate public by using following formula..

Destination public key= Gb mod Pl

After completion of public key generation process the destination node will send the public key to source node. The source node will retrieve public key and calculate secret or shared key by using following formula.

Shared key= destination public key a mod P

The destination node will take source node public key and calculate secret or shared key by using following formula.

Shared key= source node pubic key b mod P

The completion of Secret key generation process the source and destination nodes are get same secret key. The completion of secret or shared key process the source node will enter transferred message and perform the encryption process. After completion of encryption process the source ndoe will transferring cipher formatted data to server. The server will retrieve cipher formatted data and generate routing from source node to destination node. The generation of routing process can be done by randomly. The implementation process of routing is as follows.

Route Discovery Phase:

In the route discovery process the source node will send cipher formatted to server and the server also will retrieve source and destination node ids. After retrieving the server will generate random routing by using following process.

The server will retrieve all distance points of each and every node.

By taking those points the server will generate distance matrix by finding difference between source nodes to other nodes by using the following formula.

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

The completion of distance matrix the server will generate random path and calculating distance of all paths by adding difference.

4 Take those difference values of all routes and calculate minimum distance the path to contain. Consider that path as shortest path and send the cipher formatted data through that path.

Before finding the shortest route the source node will enter message and perform encryption, decryption process. The encryption and decryption process can be done by using prime order key xor cryptography technique. The implementation of encryption process is as follows.

Message Encryption Process:

P=plain Text

Take plain format message or text and add the randomized characters in between the plain text. The insertion of random character can be by every 3 characters.

Take those duplicated added character set and get the decimal values of each characters.

Take those decimal and Convert those values into Binary format.

Perform the once Complement until length of duplicated character added data.

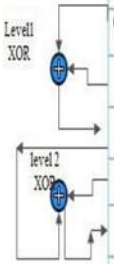
Generate prime numbers that could be contain length of duplicated data set and convert those primary number into Binary format.

After completion of binary format take those binary formatted data and perform the first level Exclusive OR (XOR) between characters of plain text and selected series of prime numbers.

After completion of first level XOR Operation and retrieve secret key.

Take first level xor data and key perform the Second level of XOR operation.

After completion of second level xor operation take those value 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 send cipher format data 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.

Message Decryption Process:

In this module the destination node will cipher formatted data and perform the decryption process.

The destination node will cipher formatted and convert into Binary format. The destination node will take secret key and convert into binary format.

After completion of conversion process the destination will perform the first level of Exclusive OR (XOR) operation between cipher text and Key.

Take those value of first level xor operation and Select the series of prime numbers and convert it into the binary format (the series must be same in both encryption side and decryption side).

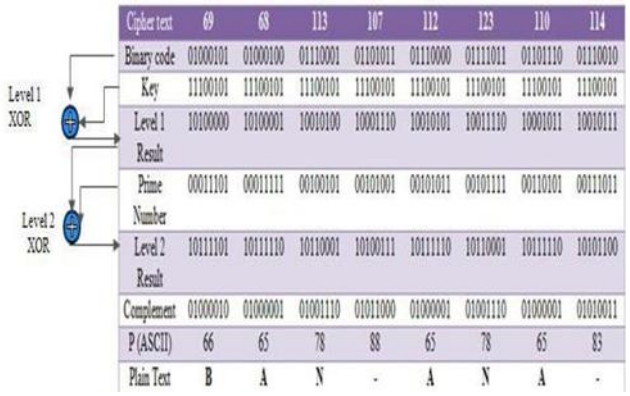
After completion of binary format do second level of XOR operation between result of step2 and selected series of prime numbers.

After completion of second level xor operation take those binary data and perform once complement.

Take those complemented data and Convert decimal format.

Take those decimal values and convert into character will get duplicated text added data. Take that data and remove the randomized added character from every there characters.

Now you can get the plaintext.



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	-

4. Conclusions

In this paper we are proposed an efficient secret randomness routing process for transferring data from source node to destination node. Before transferring data from source node to destination node we are generating common secret key. By using that key the source node and destination node will perform the encryption and decryption process. 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. After completion of encryption process the source node will transferred cipher format data to destination node through server. The server will retrieve cipher format and 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

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

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

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

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

Mukesh Singhal, 2012. “Key Management Protocols for Wireless Networks“international journal.

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.

Renner and S. Wolf, 2005. “Simple and Tight Bounds for Information Reconciliation and Privacy Amplification”,pp: 199-216.

Ren, K and Q. Wang, 2011. “characteristics in wireless communications,” Wireless Communications, IEEE, 18(4): 6-12.

Sunar, B., 2009. “True random number generators for cryptography,” in Cryptographic Engineering. Springer, pp: 55-73.

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

Ueli M. Maurer, 2011. “Secret key Agreement By Public discussion from common Information” IEEE Transaction, March.

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.

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.

P.Sri Ram Chandra,G.Venkateswara, G.V.Swamy, ‘Ultramodern Encryption Standard Cryptosystem Using Prolic Series for secure data transmission’’ ,International Journal of Latest Engineering Research and Applications(IJLERA)ISSN 2455-7137 Volume_02,Issue 11,November-2017,pp-29-35.

P. Sri Ram Chandra, G. Venkateswara, G .V.Swamy, “Modular Encryption Algorithm for Secure Data Transmission ”, Int .J. Sc.Res. in Network security and Communication ,ISSN:2321-3256,volume 6,Issue-1,February 2018