A Novel Secret Common Randomness Routing and Secrecy Data Sharing in Ad hoc Network

Gundala Pallavi[1], K. Jagdeeshwara Rao [2]

Final M.Sc. Student[1], Lecturer [2]
[1, 2] M. Sc Computer Science, Chaitanya Women's PG College, *Old Gajuwaka, Visakhapatnam 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: *Dynamic Source Routing, Security, Secret Key Establishment, Common Randomness.*

I. INTRODUCTION

A mobile ad hoc network is a collection of hundreds and thousands of low cost and low power mobile nodes connected by wireless links.[1] In operation, the nodes of a MANET do not have a centralized administration mechanism. It is known for its routable network properties where each node act as a "router" to forward the traffic to other specified node in the network. MANET is a self-configuring network of mobile routers connected by wireless links with no access point. Every mobile device in a network is autonomous. The mobile devices are free to move and organize themselves arbitrarily. Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically 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 work helps to improve the throughput and to reduce the packet loss and packet delay. It also increases the packet delivery ratio. This research work proposes an Energy Entropy-based minimum Power cost Multipath routing algorithm in MANET. It is used to increase the reliability of data transmission. The multipath routing protocols are used to reduce the routing overhead, delay and to increase the data rate. The On-Demand routing protocols discover the paths only when it is required to communicate with other nodes. The minimum-hop maximum-power routing can significantly reduce the energy consumption time.

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.[2]The proposed work helps to improve the throughput and to reduce the packet loss and packet delay. It also increases the packet delivery ratio. This research work proposes an Energy Entropy-based minimum Power cost Multipath routing algorithm in MANET. It is used to increase the reliability of data transmission. The multipath routing protocols are used to reduce the routing overhead, delay and to increase the data rate. The On-Demand routing protocols discover the paths only when it is required to communicate with other nodes. The minimum-hop maximum-power routing can significantly reduce the energy consumption time.

MANET establishes secret common randomness between two or multiple devices in a network that resides at the root of communication security. [3] In its most frequent form of key establishment, the

problem is traditionally decomposed into a randomness generation stage and an information agreement stage, which relies either on public-key infrastructure or on symmetric encryption. It relies on the 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 networks are highly dynamic and largely unpredictable. The randomness is usually evident in easily accessible networking metadata such as traffic loads, packet delays or dropped- packet rates. 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

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. 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 (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. 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 (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. 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.

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.

Nodes initiation process:

In this module we are generating communication process of each node to server. Before performing all three concepts we are generate communication of each node. The communication process can be done by sending ip address and port number of server. After sending request the server will accept the request and generate communication between nodes. 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.

Secret Key Generation Process:

1. The source node and destination node will choose two prime numbers P and G.

2. The source node will enter private key (a) and generate public key by using following formula.

Public key = $G^a \bmod p$

3. After generating public key the source node will send to destination node.

4. The destination node will retrieve public key and the destination node will enter private key(b) calculate the public key.

Destination public key= G^b mod Pl

5. The destination node will send the public key to source node 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 completion of this process the source node and destination node will get same type of secret key. The completion of secret key the source node will enter transferred message and perform the encryption process. After transferring 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.

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 points of individual clients.

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

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

3. The calculating difference we can generate random path and calculating distance of all paths by adding difference.

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

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

Encryption:

P=plain Text

1. Add the randomized characters in between the plain text. For every 3 characters add one duplicate character.

2. Get the ASCII codes for the characters in plain text.

3. Convert the ASCII codes into Binary format.

4. Do the complement of the plain text.

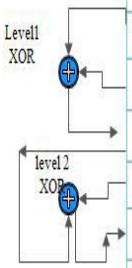
5. Select any series of prime numbers and convert into Binary format.

6. Do the first level Exclusive OR (XOR) between characters of plain text and selected series of prime numbers.

7. Select any Randomized number (key). Get the key th prime number from the prime numbers table.

8. Do the Second level of XOR operation between result of step5 and Randomized prime number.

9. Convert the result of step7 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

After 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.

Decryption:

1. Convert the cipher text into Binary format. Get the Key th prime number from the prime numbers table. And convert it into binary format.

2. Do the first level of Exclusive OR (XOR) operation between cipher text and Key th primary key.

3. 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).

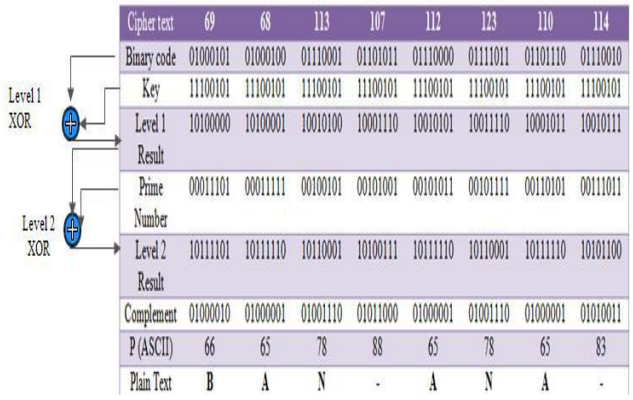
4. Do second level of XOR operation between result of step2 and selected series of prime numbers.

5. Get complement of the result of step4.

6. Convert the result from binary to decimal format.

7. Remove the randomized stuffed numbers.

8. 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	-

IV. 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

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

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

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

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

[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].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.

BIOGRAPHIES:

Gundala Pallavi is student in M.Sc. (Computer Science) in Chaitanya Women's pg college, Old Gajuwaka, Visakhapatnam. She has received his Degree B. Sc (MPCS) from M.V.R Degree College, Chinagantayada, Visakhapatnam. Her interesting areas are data mining, network security and cloud computing.

K.Jagdeeshwara Rao is working as a Lecturer in Chaitanya Women's pg college, old Gajuwaka, Visakhapatnam Andhra Pradesh. He received his M.Sc. (Computer Science) from Gayatri Vidya Parishad, Andhra Pradesh. His research areas include Network Security and Computer Networks