Privacy Preserving of Information sharing system for Human Networks

Gatta Pushpa[1], Sri Lakshmi Kanagala[2],

Final M.Tech Student [1], Associate Professor[2]
[1,2]Department of Computer Science & Engineering, Dadi Institute of Engineering & Technology, Anakapalle- 531 001, A.P.

Abstract: *Now a day's sharing information of mobile devices are becoming necessary of our daily lives. So that sharing information using existing mobile device technology rely on efficiency of internet and also increase time complexity. Because by using existing technology to transfer sharing data through server. This architecture is inefficient in many situations and also does not utilize abundant inter device communication opportunities in many scenarios. This paper proposed the inter device network for direct interactive with mobile device. By implementing this architecture each device not communicate with centralize device. The communication process can be done by using inter device network for sharing information. In this paper we can also provide security of transferring data by using prime order complement data cryptography technique for data encryption and decryption. By implementing those techniques we provide more efficiency of internet and also provide more security of transferred data.*

Keywords: *Security, routing, cryptography, wireless network.*

I. Introduction

Today's wireless technology is fast growing for consumer demands and becoming a necessary for part of our life. By implementing wireless technology we can share information from one place another place. In a wireless technology only allows mobile device to communicate with each other for sharing information. By implementing wireless technology so many architecture are available in the networks. In the existing architecture are fails for many situations due to limited number of resources. For example of taking conference room, the mobile device connection can be disabled; because of the so many devices is connection to wireless network. In the wireless network technology another disadvantage is that inter device communication. By implementing inter device communication we can reduce burden of server. By performing this functionality we can improve network efficiency and also satisfy the consumer demands.

Now a day's most of the wireless technology can't be used for sharing of information. By implementing wireless technology the mobile device also sharing images, videos and music stream services. So that by performing this functionality the existing architecture of wireless network is inefficient in many scenarios. Because in the existing architecture all devices are connect to central service provider, which will fail in many situations. So that by overcome those problem we can implement new architecture is networking portable wireless device. This architecture also called delay tolerant network [1]. By implementing this type of architecture we can adopt store carry and forward model. So that by implementing this architecture we can expand communication capability of mobile devices. By combing new architecture of delay tolerant network and some of the limitation of existing architecture we can implement new dynamic approach is human networks. By implementing this architecture we can provide short range mobile device communication can be provide. So that the sharing information completely done by using decentralized manner. So that by implementing human networks we can reduce burden of central service provider.

In this paper we are implementing one of architecture of human network for sharing information from source node to destination node. By implementing this process the central service provider will only find the routing from source node to destination node. After that the routing path will sent to source node, destination node and inter device communicator. By using that path the inter device communicator will sent information from source node to destination node. So that by implementing this process we can reduce some of burden of central service provider. Before finding the path from source node to destination the central service provider also send node information to inter device communication. Before sharing information through network it will provide privacy of sharing information. By providing privacy of sharing information we are implementing one of the concepts of cryptography. In this paper we are implementing one of the cryptography for encryption and decryption of sharing information.

By providing security of transferring message each source node will encrypt the message and sent

to destination node. The destination node will retrieve the cipher formatted data and decrypt cipher data, get the original message. So that by implementing this cryptography technique we can provide more security of transferring data and also improve efficiency wireless network. In the cryptography technique the transferring message to unknown format is encryption process. By implementing of reverse process is called decryption process. The remainder of this paper is organized as follows: Section 2 presents the related work of our proposed system. Section 3 is to specify existing system architecture. Section 4 is to specify implementation procedure of our proposed system. Section 5 presents the result analysis of our proposed system. Section 6 analyzes to the conclusion our proposed system. Section 7 is to specify the reference of our proposed system.

II. RELATED WORK

By implementing the human network it follows the architecture for utilizing store-carry-forward communication paradigm for sharing of information in wireless sensor network. One of the important feature of human network that is different from delay tolerant network that is inherent it social network structure. The design and analysis of human network contact reveals that communication for information sharing through the network by providing the routing [2][3][4][5]. In the previous work [7][6] we are implementing optimal
Forwarding rule based is used sharing of information in a long term relationship between users. By implementing all of these routing techniques requires stable contact patterns and need to pre-process to gather routing information. By performing those concepts it will take more time for finding routing information of source node to destination node. Another concepts is content based is interest driven for data diffusion applications [8].

In the wireless network another important issue for provide security [9][10][11]of transferring message. By providing privacy of shared data we can implement the concepts for content based pub/sub system [12]for wireless sensor network. The authors in [13] presented an analysis of the pub/sub systems in wireless mobile networks. Except for the content-based approach, there are topic/channel-based pub/sub systems that support only a limited number of communication channels [14]. Low energy processor units [15], [16] are an important enabling technology to HUNETs. A survey of the application of the Bloom filter in computer networks is in [17].

III. EXISTING SYSTEM

Existing wireless networking technologies only allow mobile devices to communicate with each other through wireless infrastructures and so on. This architecture, however, is not ubiquitously applicable. First, it fails in many situations due to limited network resources. For example, in a conference room, the Wi-Fi and cellular connection can be crippled because too many users are competing for the channel simultaneously. Second, this architecture does not take advantage of the abundant inter device communication opportunities. Again, take the conference room scenario as an example; because of the high density of wireless devices, there can be excellent wireless connections between nearby mobile devices. Existing wireless networks are unable to utilize such communication opportunities. As a result, this architecture fails to address novel application requirements. Nowadays, most mobile applications are for information sharing; mobile devices are increasingly becoming the end points of information consuming. Evidence is that almost all existing smart phones and tablets are integrated with vendor-supplied music/video streaming services, and social-network-based information sharing services are extremely popular on mobile devices. Given the existing architecture, however, they have to connect with central service providers, which would fail in many situations as described above. Besides, this architecture can be inefficient in many scenarios.

IV. PROPOSED SYSTEM

In this paper we are using inter device network for sharing information through the mobile devices. By implementing inter device network communication we provide routing and transfer sharing data. Here the finding routing can be done by central application provider and transferring data by inter device network. Before finding routing of device the centralized application server will perform following process.

1. Each node or mobile device will send request for communication process.

2. After sending request the centralized server will accept request and send id (U_i) and signal strength (S_i) of each device. Before sending signal strength of each device the centralized server also generates each channel capacity (C_i) and store into data base.

3. The centralized server will find the routing of send node to receive node based cost matrix. The generation of cost matrix can be done by using following formula.

Channel capacity= $C_1 + C_2 + \ldots\ldots +$

Signal strength=$S_1 + S_2 + \ldots\ldots + S_i$

Total Capacity= S_i+C_i

Cost matrix=total capacity-(S_i+C_i)

4. After generation cost matrix the centralized server will find out route from send node to destination node by performing following procedure.

i) Finding routing of source node to destination node by using cost matrix.

ii) finding we can find out minimum distance of each source node to other nodes based cost matrix. Likewise we can generate routing of source node to destination.

5. After finding routing from source node to destination node the centralized sever will send that path to inter device network and also send to both nodes.

After sending path to specified sender and receiver nodes, sender node will transfer information through specified path and transferring data by using inter device network. Before transferring data the sender node will encrypt shared information by using encryption process prime order complement cryptography technique.

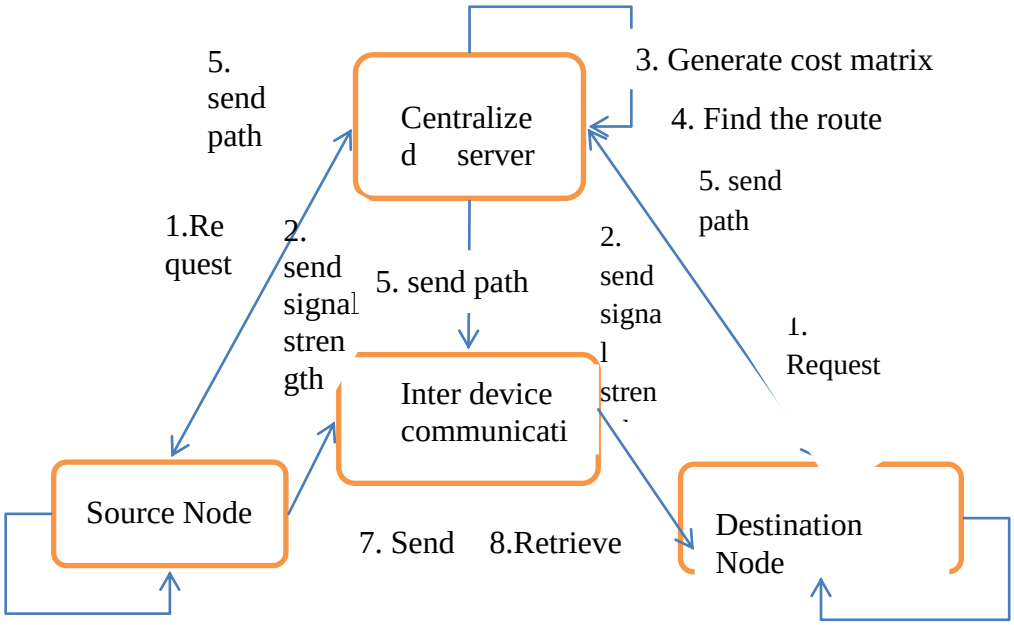
Encryption process of Prime order complements cryptography technique:

1. Read each character from the transferring message and convert into ascii format.

2. Generate random prime number based on length of transferring message.

3. After converting ascii values xor with prime numbers until length of message.

4. After performing xor operation those values can convert into binary and revers those binary values.



5. Take the reverse binary values and get two bits first binary values and perform following operation until length message completed. Here 4 distinct blocks, according to the order they are 01, 00, 10, 11. So we put according to key generation technique 01=a, 00=b, 10=c, 11=d that is 1st level identification marks. For the generation of 2nd level identification marks, again the two bit representation of a, b, c & d is aa, ab, ac, ad, bb, bc, bd, cc, cd, dd,

ba, ca, da, cb, db, dc. Now we put aa=e, ab=f, ac=g, ad=h, bb=i, bc=j, bd=k, cc=l, cd=m, dd=n, ba=o, ca=p, da=q, cb=r, db=s,dc=t.

6. After performing second level those value are cipher data. The cipher data will be sent to specified destination node through given path.

Decryption process of Prime order complements cryptography technique:

The destination node will retrieve cipher format data and decrypt the cipher data by performing the following steps.

1. The destination node retrieve cipher data and again perform the second level process i.e. e==aa, f=ab, g=ac, h=ad, i=bb, j=bc, k=bd, l=cc, m=cd, n=dd, o=ba,p= ca,q= da,r= cb,s= db, t= dc.

2. after getting value of a,b,c and d we can get those value of bit values and form the eight bit length of string.

3. Take those eight bit length strings and reverse those values.

4. After reverse the values we can convert into ascii format.

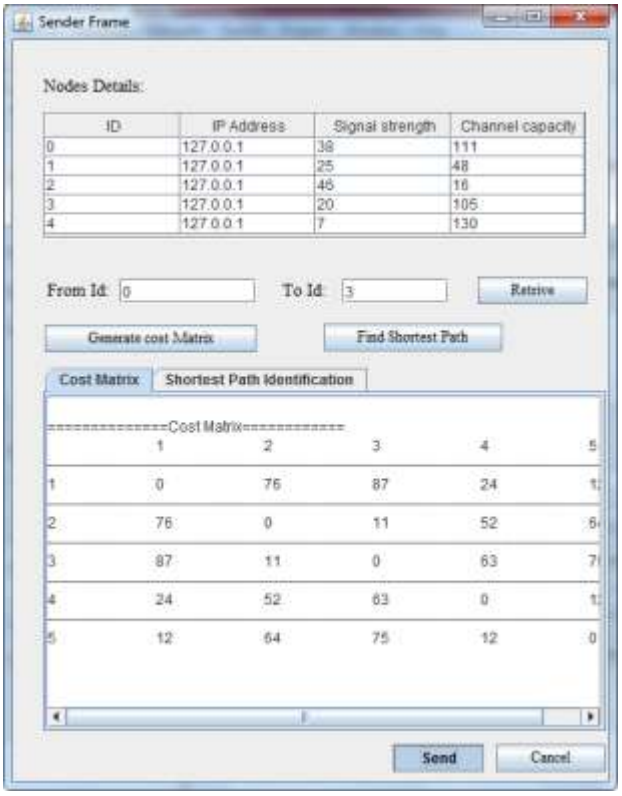
5. Take those ascii value and xor with prime number we can get xored values.

6. by performing xor operation we can get original message.

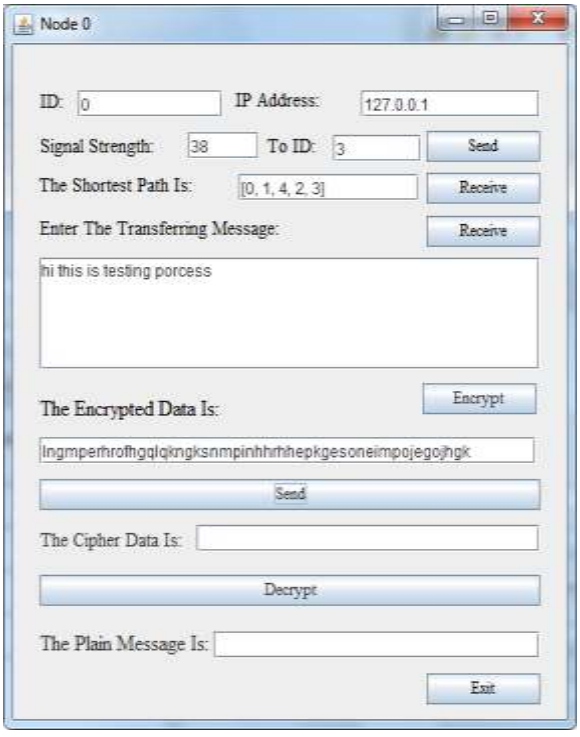
In the network if any user wants to perform the encryption and decryption process. In this paper we are using transferring messages can be sent through the inter device communication. So that by implementing this process we can improve the efficiency human networks and also provide more privacy of transferring message.

V. EXPERMENT RESULT

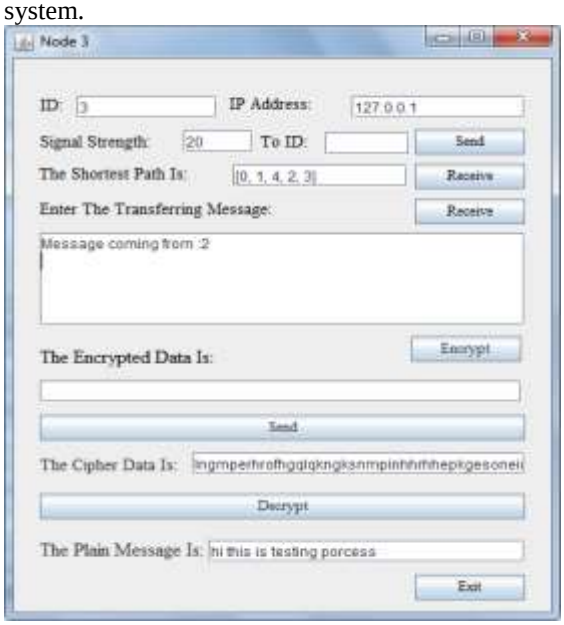
In this section we can describe experiment result of our proposed system. By specifying this section we can mention what type of result can show by implementing the proposed system. In this paper we are using java language for performing the functionality of proposed system.



The above diagram specify all details of nodes availbe in the human netwoks. This diagram also contains information about signal stregth and channel capacity of each node in the network. This diagram also maintain generation of cost matrix and using this matrix we can findout routing from source node to destination node.



The above diagram specifies functionality of source node in the network. Each source node will retrieve their ids from central service provider and also get signal strength. After getting the source node will choose destination id and send to central service provider. The central service provider will find out routing from source node to destination node and sent that routing path to both nodes. Both nodes will retrieve the routing path and sent message through that path. Before sending information to destination node the source node will convert that information to unknown format by using proposed system.



The above diagram specifies functionalities of destination node. The destination node will also maintain same type of information that can be maintained by the source node. So that the destination will retrieve the cipher format data from the source node and decrypt that data by using the decryption process of proposed system. After performing decryption porcess we can get original message.

VI. CONCLUSION

In this paper we proposed an inter device network architecture used for sharing information in a mobile device. So that by providing this architecture we can improve efficiency of internet service for sharing data in the mobile devices. Specifically in this architecture we are using inter device communication for sharing information in mobile devices. In this paper we can also provide concept for cryptography of data security. By implementing those concepts we can improve efficiency of internet service and also provide privacy of transferring data.

VII. REFERENCES

[1]. K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. Conf. Applications, Technologies, Architectures, and Protocols for Computer Comm., pp. 27-34, 2003.

[2] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Pocket Switched Networks: Real-World Mobility and Its Consequences for Opportunistic Forwarding," IEEE J. Selected Areas Comm., vol. 26, no. 5, pp. 748-760, Feb. 2005.

[3] A. Chaintreau, P. Hui, C. Diot, R. Gass, and J. Scott, "Impact of Human Mobility on Opportunistic Forwarding Algorithms," IEEE Trans. Mobile Computing, vol. 6, no. 6, pp. 606-620, June 2007.

[4] C. Qian and S. Lam, "Greedy Distance Vector Routing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), pp. 857-868, June 2011.

[5] S.S. Lam and C. Qian, "Geographic Routing in D-Dimensional Spaces with Guaranteed Delivery and Low Stretch," Proc. ACM SIGMETRICS Joint Int'l Conf. Measurement and Modeling of Computer Systems (SIGMETRICS '11), pp. 257-268, 2011.

[6] Y. Zhao and J. Wu, "B-Sub: A Practical Bloom-Filter-Based Publish-Subscribe System for Human Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS '10), pp. 634-643, 2010

[7]. C. Liu and J. Wu, "An Optimal Probabilistic Forwarding Protocol in Delay Tolerant Networks," Proc. MobiHoc '09, pp. 105-114, 2009.

[8] I. Carreras, D.P. Francesco, D. Miorandi, D. Tacconi, and I. Chlamtac, "Why Neighborhood Matters: Interests-Driven Opportunistic Data Diffusion Schemes," Proc. Third ACM Workshop Challenged Networks (CHANTS '08), pp. 81-88, 2008.

[9] W. Fang, F. Liu, F. Yang, L. Shu, and S. Nishio, "Energy-Efficient Cooperative Communication for Data Transmission in Wireless Sensor Networks," Consumer Electronics, IEEE Trans., vol. 56, no. 4, pp. 2185-2192, Nov. 2010.

[10] Y. Li, D. Jin, L. Su, and L. Zeng, "Stability and Scalability Properties for Dynamic Content Updates over Delay Tolerant Networks," Proc. 20th Int'l Conf. Computer Comm. and Networks (ICCCN '11), pp. 1-6, Aug. 2011.

[11] G. Sollazzo, M. Musolesi, and C. Mascolo, "TACO-DTN: a Time- Aware Content-Based Dissemination System for Delay Tolerant Networks," Proc. ACM First Int'l MobiSys Workshop Mobile Opportunistic Networking (MobiOpp '07), pp. 83-90, 2007.

[12] T. Pongthawornkamol, K. Nahrstedt, and G. Wang, "The Analysis of Publish/Subscribe Systems over Mobile Wireless Ad Hoc Networks," Proc. ACM Fourth Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '07), pp. 1-8, Aug. 2007.

[13]A. Carzaniga, D.S. Rosenblum, and A.L. Wolf, "Content-Based Addressing and Routing: A General Model and its Application," 2000.

[14] P.T. Eugster, P.A. Felber, R. Guerraoui, and A.M. Kermarrec, "The Many Faces of Publish/Subscribe," ACM Computing Surveys, vol. 35, no. 2, pp. 114-131, 2003.

[15]. [28] W. Hu, J. Wang, X. Gao, Y. Chen, Q. Liu, and G. Li, "Godson-3: A Scalable Multicore Risc Processor with X86 Emulation," Micro, IEEE , vol. 29, no. 2, pp. 17-29, Mar.-Apr. 2009.

[16] W. Hu, R. Wang, Y. Chen, B. Fan, S. Zhong, X. Gao, Z. Qi, and X.Yang, "Godson-3B: A 1 ghz 40 w 8-Core 128 gflops Processor in 65 nm cmos," Proc. IEEE Int'l Solid-State Circuits Conf. Digest of Technical Papers (ISSCC '11), pp. 76-78, Feb. 2011.

[17] A. Broder and M. Mitzenmacher, "Network Applications of Bloom Filters: A Survey," Internet Math., pp. 636-646, 2002.

BIOGRAPHIES:

Gatta Pushpa is student in M.Tech(CSE) in Dadi Institute of Engineering & Technology, Anakapalle, Visakhapatnam.She has received her B.tech(C.S.E) from Dadi Institute of Engineering & Technology, Anakapalle, Visakhapatnam. Her interesting areas are computer network and operating system.

Sri Lakshmi Kanagala is working as a Associate professor in Dadi Institute of Engineering & Technology, Anakapalle, Visakhapatnam, Andhra Pradesh. She received her degree Master of Technology in Computer Science & Engineering from Andhra University, Visakhapatnam. Her research areas include Operating Systems, Computer Networks.