Security in Opportunistic Network

Harshal S. Patil[1], Ajay P. Patil[2], Akshay V. Pathak[3], Jitendre P. Chaudhari[4]

U.G. Students
Department of Computer,
SSBT's COET, Jalgaon, India

***Abstract*— The emergence of extremely powerful mobile communication devices in recent times has triggered off the development of many exploitative technologies that attempt at leveraging the ever increasing processing, storage and communicating capacities of these devices. One of the most developing area of network is opportunistic network. It provides communication even in disconnected mode. Nodes are mobile and can change their location and message is forward through many intermediate nodes so identity of users is shown to all.**

Any intermediate can drop the data packets if he is not wishes to forward the data to a particular destination id. A few privacy preventing algorithms are proposed to maintain it. In this research we propose an algorithm to maintain the privacy of user if user wants it . We are ensuring the privacy of
the data with the use of concept of encrypted key. In this we use the symmetric key cryptography technique for data encryption and decryption.

***Index Terms*— Privacy, Opportunistic Network, Encrypt, Cryptography.**

I. INTRODUCTION

Opportunistic networks is a type of challenged networks. An opportunistic network is a sub-class of delay tolerance network where communication contacts are not constant, so an
end-to-end path between the source and the destination may never exists. An opportunistic network may include cellular Base Stations (BSs), offering macrocell (macroBS), microcell,
picocell, or femtocell (femtoBS) coverage, as well as WiFi access points (APs), mostly connected through wireless networks. In opportunistic networks each node acts as a gateway which makes it much more flexible than DTNs.
The opportunistic networks (OppNets) are characterized as a most challenging evolution of Mobile Ad-Hoc Networks (MANET). OppNet provide possibility to exchange messages between mobile nodes (users) even in such a disconnected environment by opportunistically selection any nearby device to move messages closer to the final nodes. The privacy that we use in opportunistic network is very different form than the privacy in opportunistic networks has been given by various researchers.

Security aspects such as confidentiality, integrity and availability can be managed in infrastructure centric networks with well known methods. The situation is however much more challenging in opportunistic networks where end-to-end trust relations are hard to build and availability by definition can be poor. However, similar approach in opportunistic networks is impossible due to the facts that there is no network infrastructure and because a node that tries to use another nodes resources can be virtually anyone. Flooding is hence somewhat challenging to prevent in opportunistic networks, although the number of effected nodes can be managed through behavior monitoring algorithms and with nonstandard routing paradigms. Because typically adjacent node trust relation is non-existing in opportunistic networks as well as in many traditional networks, all the data has to be encrypted on the originating node and decrypted on the destination node to satisfy the data integrity and confidentiality aspects of the security. This means that there has to be means to authenticate other users, or otherwise user identities can not be verified and sybil attacks are possible.

The Security In Opportunistics network has been proposed in this paper with its algorithm, result, technical discussion and conclusion.

II. ALGORITHM

The Advanced Encryption Standard (AES) algorithm will encrypt and decrypt the text to provide security. The existing algorithm is having complex design and can be hacked. To overcome this issue concept of encrypted key is used along with the AES algorithm.

A. Encryption Algorithm

Step 1) Declaration of Header

Step 2) Declaration of variables character array ap, d, c, aq. Byte array b, key, key1. String variables s, t, line. Secret Key variables secretKey, app for storing key in Secret Key format.

Step 3) Read the message from user and store it into line variable.

Step 4) Generate 128 bit secret key using AES algorithm and store it in secretKey variable. Convert that secret key into string format and store it in string variable s. Transform string in s variable into character array and store it in character variable d. Reverse that string in s variable and store it in character array variable c.

Step 5) Apply XOR operation on character arrays d and c and store the result in string variable t. Convert that string in t into secret key format and store it in secret key variable app.

Step 6) Apply the encryption on text in line variable using secret key in app variable and store result in textEncrypted variable.

Step 7) Print encrypted cipher text message and send it to destination side along with main secret key.

Step 8) End

B. ***Decryption Algorithm***

Step 1) Declaration of Header.

Step 2) Declaration Declaration of variables character array ap, d, c, aq. Byte array b, key, key1. String variables s, t, line. Secret Key variables secretKey, app for storing key in Secret Key format.

Step 3) Apply the XOR operation on secret key came from sender and generate encrypted key.

Step 4) Apply the decryption on cipher text came from sender using encrypted key and store the result in textDecrypted variable.

Step 5) Print decrypted text message and check whether it is same as original text or not.
Step 6) End.

III. RESULT

During communication sender sends the original text message and encryption algorithm applied on the message then the original message is split into two parts cipher text and private key. By applying XOR operation on private key, encrypted key is generated and by using that encrypted key the original message is encrypted and then cipher text and private key are transferred to receiver. At receiver side, both the cipher text and the private key are merged using decryption algorithm and using same XOR operation as in sender side, here also encrypted key is generated from private key and then original message is obtained from cipher text. Here AES (Advanced Encryption Standard) encryption algorithm is used for generation of private key.

The following table shows encryption and decryption of various inputs like number, symbol, text, capital letters, small letters etc.

Type of Input	Input Text	Cipher Text	Symmetric Key	Output Text
Number	0123456789	j/iC1tzwjmc Yq8SZL20qkg==	+MpGO/BlFUR xlPjPHaYwRg==	0123456789
Symbol	, . !@?	8C81+BgIq5X qadZoyLVpcA==	OK89sRhyO2g DEL1728FZmg==	, . !@?
Text	Hello World	/VExzSU1POP z9ruLGRUONA==	hkUhDt8Ush OcFdlS8sOaAA==	Hello World
Capital Letters	ABCDEFG	gYerqSuOBi cI1x3xajhvRA==	jMU2MRom6vS VpVGo6a+99w==	ABCDEFG
Small Letters	abcdefg	WX1YIqGCPK rkfF33nZmvqQ==	9c5pJHFOKob hIA2bqXjn7g==	abcdefg

Fig. 1 Result of various Inputs

As per given table every time for each input text new 128 bit AES symmetric key is generated which is very secured. Then by reversing this key and applying XOR operation on original key and reversed key new encrypted key is generated. Using this encrypted key input text is encrypted and cipher text along with AES symmetric key is send towards destination. At the

destination side same XOR logic is applied to obtain same encrypted key as on sender side. Then after generating encrypted key at destination side original text is obtained from cipher text.

IV. DISCUSSION

Previous opportunistic network systems focuses on node security, node authentication and how reliably data should reach at the destination. They also focuses on maximum data delivery towards the destination. But data security is not taken under consideration that is data is not in encrypted form when it is generated at the source. So our proposed system provides data security in the form of encrypted data at sender side using AES encryption algorithm. This encrypted data is transmitted towards the destination and only authenticated user/node can decrypt that encrypted data to get original data using AES decryption algorithm.

V. CONCLUSION AND FUTURE SCOPE

Opportunistic network is very useful if privacy is maintained. Due to inefficiency in privacy, many false node or selfish nodes in this network do not want to forward the data to the destination. This results the increase in packet loss and decrease in throughput. To reduce the packet loss and increase the throughput, given solution proposes a network architecture in which a node want to send a message to a destination and he doesn't want to explore his identity as well as destination identity. For maintaining the privacy of data this paper introduces the concept of an encrypted key instead of main key. An encrypted key is provided for encryption of message to the source and for decryption of the message at the destination side maintaining the confidentiality of the message. The symmetric cryptography technique is used for data encryption and decryption. This approach provides privacy to the user and reduces the packet loss by a selfish node.

The proposed technique provide privacy to the data in opportunistic network on the basis of providing unique id by a stable node, which is present in every cluster. But this technique increases the work load of a sender who wishes to communicate. In future our research tries to add a way which reduces the user work by providing some new mechanism to hide the unique id of user. Due to infrastructure less architecture and mobility of the nodes, opportunistic network faces many problems related to security, privacy, nodes authentication and efficient routing protocol.

REFERENCES

[1] Er. Maggi Goyal, Er. Manoj Chaudhary, “Ensuring Privacy in opportunistic Network ”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 13, Issue 2 (Jul. - Aug. 2013), PP 74-82.

[2] Anna Scaglione Opportunistic Large Arrays: Cooperative Transmission in Wireless Multihop Ad Hoc Networks to Reach Far Distances IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 51, NO. 8, AUGUST 2003.

[3] Zehua Wang CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 30, NO. 2, FEBRUARY 2012.

[4] Abdullatif Shikfa and Melek nen and Re_k Molva Local key management in opportunistic networks Int. J. Communication Networks and Distributed Systems, Vol. 9, Nos. 1/2, 2012.

[5] Enrico Scalavino, Giovanni Russello and Rudi Ball An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios ASIACCS10 April 1316, 2010, Beijing, China.

[6] Pelusi, L., Passarella, A. and Conti, M. (2006) Opportunistic networking: data forwarding in disconnected mobile ad hoc networks, IEEE Communications Magazine, Vol. 44, pp.134, 141.