IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 13, Issue 2 (Jul. - Aug. 2013), PP 74-82
www.iosrjournals.org

Ensuring Privacy in opportunistic Network

Er. Maggi Goyal[1,] Er. Manoj Chaudhary[2]
[1]*Research Scholar, Computer Science, Yadavindra College,Talwandi Sabo,Punjab,India.*
[2]*Lecturer,Computer Science, Yadavindra College,Talwandi Sabo,Punjab,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 usersis shown to all.Any intermediate can drop the data packetsif 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 cluster estimation. In this we use the public private cryptography technique for data encryption and decryption. Algorithm is implemented on NS2 (Network Simulator 2.35).*
Keywords: *Attacks, Virtual ID, Privacy, NS2*

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. The devices included in an opportunistic network can be mobile phones, personal computers, cameras, etc. In opportunistic networks each node acts as a gateway which makes it much more flexible than DTNs. Now the most basic question arises i.e. what is DTN network? How opportunistic network is different from mobile adhoc networks(MANETs)?

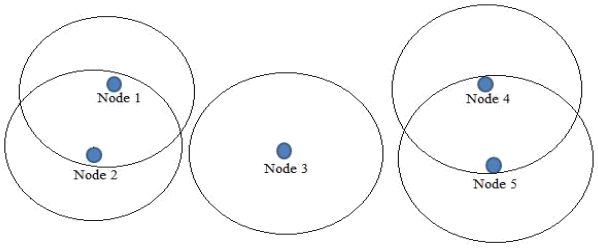

Figure 1 An Opportunistic Network

In Fig 1, Node 3 does not know the existence of Node 1 or Node 2 and Node 4 or Node 5, since they are not within its communication range. Node 1 and Node 2 do know of each other and are able to communicate. Similarly, Node 4 and Node 5 are also know each other and are able to communicate. Many opportunistic forwarding protocols are replication based. The replication factor depends on a heuristic which is used by intermediate nodes to decide either to forward the message or to drop it[7]. There are many examples of such networks in real life. For example, in north part of the Sweden[16], the communication between villages and the summer camps of the Saami population is provided when the nodes get connected. The same situation is also seen in rural villages of India and some other poor regions[17]. Other fields where this kind of communication scenarios may occur also include satellite communication[18], wildlife tracking[19], military networks[20] and vehicular ad hoc networks[21]. Ad hoc network is a decentralized type of wireless network. In ad hoc network there is no pre-existing infrastructure, such as routers in wired networks or access points in wireless networks. In ad hoc network each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. Basically it's a network which is used in emergency causes. Here is No fixed infrastructure in ad hoc network like base stations. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other

nodes to relay messages. Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. The lack of end-to-end connectivity is a key difference between such networks and mobile ad-hoc networks (MANETs)[8].

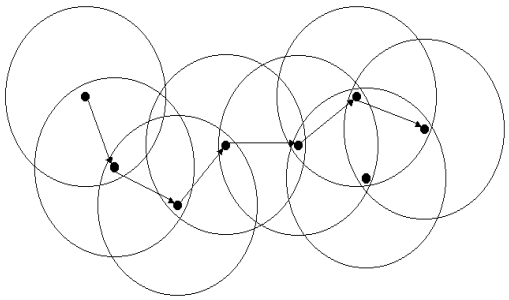

Figure 2: Mobile Adhoc Network

The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. A passive insider can attempt to track other nodes' movements by linking different location announcement messages. An active insider can modify, inject, and replay "genuine" messages[10]. Fig 2 shows the mobile adhoc network.

DTN is Delay Tolerant Network an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. The end-to-end path between source and the destination in DTNs is very low. Its is also referred as Intermittently Connected Mobile Networks. In delay tolerant network some problems are included in which lack of infrastructure and nodes are stationary are the main ones. In delay tolerant network routes are time dependent and requires long term storage. In Security of DTN routing, encrypted methods cannot detect packet drops in the malicious node[22]. The researchers have found the problem of Selfishness in Opportunistic networks[6]. Some main problems of opportunistic networks are given below.

1. Disclosure of the message content enabling it to be access by the malicious node or the parties which are not suppose to be read it.
2. Data is travel from many intermediate node, so there may be a threat to the integrity of the data.
3. Protection of transmitted messages in transit for malicious purposes e.g. for masquerading .

The Opportunistic network has the following features:-

- They are governed by operators through the provision of resources (e.g., spectrum available) and policies, as well as context/ profile information and knowledge, which is exploited for their creation/maintenance.
- They are extensions of the infrastructure that will include various devices and terminals potentially organized in an infrastructure-less mode, as well as elements of the infrastructure.
- They will exist temporarily, i.e. for the time frame necessary to support particular applications (requested in specific location and time). Applications can be related to the social networking and prosumer (derives from the combination of "producer" and "consumer") concepts as well as to the support of an enterprise (in a particular area and time interval) for developing and delivering products or digital services.
- At the lower layers, the operator designates the spectrum that will be used for the communication of the nodes of the opportunistic network (i.e. the spectrum derives through coordination with the infrastructure). In this respect, in principle, the bands will be licensed.
- The network layer capitalizes on context-, policy-, profile-, and knowledge-awareness to optimize routing and service/content delivery.

There are also different types of attacks in opportunistic networks:-

A) Worm Attack
B) Viruses Attack.

Viruses Attack:- A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or

program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

Worms Attacks:- Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

II. Background And Related Work

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.

A. Routing Protocols in Opportunistic Network

A.1 Anna Scaglione in year 2003 proposed a technique called Opportunistic Large Array for sending the data to very long distance this technique allows efficient flooding of a wireless network with information from a source, which we refer to as the leader. At the same time, it permits us to transmit reliably to far destinations that the individual nodes are not able to reach without consuming rapidly their own battery resources, even when using multihop links (the reach-back problem). The synchronization constraints are extremely loose and can be fulfilled in a distributed manner. The key idea is to have the nodes simply echo the leader's transmission operating as active scatterers while using adaptive receivers that acquire the equivalent network signatures corresponding to the echoed symbols. The active nodes in the network operate either as regenerative or nonregenerative relays. The intuition is that each of the waveforms will be enhanced by the accumulation of power due to the aggregate transmission of all the nodes while, if kept properly under control, the random errors or the receiver noise that propagate together with the useful signals will cause limited deterioration in the performance. The avalanche of signals triggered by the network leaders form the so-called opportunistic large array (OLA)[1].

A.2 Chiara Boldrini, Marco Conti, Andrea Passarella proposed a technique for routing and forwarding in opportunistic network in year 2008 Opportunistic networks allow content sharing between mobile users without requiring any pre-existing Internet infrastructure, and tolerate partitions, long disconnections, and topology instability in general. In this paper they propose a context-aware framework for routing and forwarding in opportunistic networks. The framework is general, and able to host various flavors of context-aware routing.

In this work they also present a particular protocol, HiBOp, which, by exploiting the framework, learns and represents through context information, the users' behavior and their social relations, and uses this knowledge to drive the forwarding process. The comparison of HiBOp with reference to alternative solutions shows that a context-aware approach based on users' social relations turns out to be a very efficient solution for forwarding in opportunistic networks[2].

A.3 Zehua Wang gives a noble approach in year 2012 for routing in opportunistic network. this paper proposed that The link quality variation of wireless channels has been a challenging issue in data communications until recent explicit exploration in utilizing this characteristic. The same broadcast transmission may be perceived significantly differently, and usually independently, by receivers at different geographic locations. Furthermore, even the same stationary receiver may experience drastic link quality fluctuation over time. The combination of link-quality variation with the broadcasting nature of wireless channels has revealed a direction in the research of wireless networking, namely, cooperative communication. Research on cooperative communication started to attract interests in the community at the physical layer but more recently its importance and usability have also been realized at upper layers of the network protocol stack. In this article, we tackle the problem of opportunistic data transfer in mobile ad hoc networks. Our solution is called Cooperative Opportunistic Routing in Mobile Ad hoc Networks (CORMAN). Nodes in the network use a lightweight proactive source routing protocol to determine a list of intermediate nodes that the data packets should follow en route to the destination. Here, when a data packet is broadcast by an upstream node and has happened to be received by a downstream node further along the route, it continues its way from there and thus will arrive at the destination node sooner[3].

A.4 J.P. Tower and T.D.C. Little proposed in 2008 Opportunistic networking is emerging as a technique to exploit chance encounters among mobile nodes, and is distinct from previously studied behaviors found in sensor and ad hoc networking research. In this paper, explore contributions in epidemic data dissemination and mobile ad hoc networks applicable to opportunistic networking, and propose an extension to prior work based on *active cures*. This scheme, called SERAC, increases the rate at which cure messages are propagated in a fragmented network for the purpose of reducing the overhead of outstanding yet incompletely disseminated messages.
Preliminary analyses demonstrate the feasibility of performance gains under the opportunistic networking model[4].

A.5 Gokce Gorbil, Erol Gelenbe proposed opportunistic communication for Emergency Support Systems in 2011and Opportunistic communications (oppcomms) use low-cost human wearable mobile nodes allowing the exchange of packets at a close range of a few to some tens of meters with limited or no infrastructure. Typically cheap pocket devices which are IEEE 802.15.4-2006 compliant can be used and they can communicate at 2m to 10m range, with local computational capabilities and some local memory. In this paper we consider the application of such devices to emergency situations when other means of communication have broken down. This paper evaluates whether oppcomms can improve the outcome of emergency evacuation in directing civilians safely. We describe an autonomous emergency support system (ESS) based on oppcomms to support evacuation of civilians in a built environment such as a building or supermarket. The proposed system uses a fixed infrastructure of sensor nodes (SNs) to monitor the environment[5].

B. Security in Opportunistic Network

B.1 B.Poonguzharselvi1 and V.Vetriselvi proposed a trusted framework for data forwarding in opportunistic network in year 2012 and Opportunistic networks are usually formed spontaneously by mobile devices equipped with short range wireless communication interfaces. The idea is that an end-to-end connection may never be present. Designing and implementing a routing protocol to support both service discovery and delivery in such kinds of networks is a challenging problem on account of frequent disconnections and topology changes. In this network one of the most important issues relies on the selection of the best intermediate node to forward the messages towards the destination. This paper presents a trust framework for opportunistic network where the nodes in the network follow the trace based mobility model. The selection of next hop to forward the data packets is based on the trust value as well as the direction of movement of node towards the destination.

The trust value is obtained from the trust framework of the data forwarding node. The direction of destination is obtained from the movement trace file that is maintained by the nodes in the network. In this proposed framework, the message is encrypted to secure both the data and path information. The effectiveness of this proposed framework is shown using simulation[6].

B.2 Abdullatif Shikfa , Melek Onen , Refik Molva proposed in year 2010 and give privacy and confidentiality in context-based and epidemic routing in opportunistic network and Autonomic and opportunistic communications require specific routing algorithms, like replication-based algorithms or context-based forwarding. In addition to confidentiality, privacy is a major concern for protocols which disseminate the context of their destination. In this paper, we focus on the confidentiality 20 and privacy issue inherent to context-based protocols, in the framework of an original epidemic forwarding scheme, which uses context as a heuristic to limit the replication of messages. We define the achievable privacy level with respect to the trusted communities assumption, and the security implications. Indeed, privacy in such an environment raises challenging problems, which lead us to a solution based on refinements of two pairing-based encryption, namely searchable encryption and identity-based encryption. This new solution enables forwarding while preserving user privacy by allowing secure partial matches in the header and by enforcing payload confidentiality[7].

B.3 Abdullatif Shikfa and Melek Önen and Refik Molva proposed in year 2012 gives a technique for securing data forwarding in opportunistic network by Local key management and Opportunistic networks are a new and specific type of mobile peer-to-peer networks where end-to-end connectivity cannot be assumed. These networks present compelling challenges, especially from a security perspective, as interactive protocols are infeasible in such environments. In this article, focus on the problem of key management in the framework of content-based forwarding and opportunistic networks. After analysing this issue and identifying specific security threats such as Sybil attacks, propose a specific key management scheme that enables the bootstrapping of local, topology-dependent security associations between a node and its neighbours along with the discovery of the neighbourhood topology[8].

B.4 Enrico Scalavino, Giovanni Russello and Rudi Ball proposed a novel approach for security in opportunistic network in year 2010 that a novel version and implementation of the Policy-based Authority Evaluation Scheme (PAES) to protect data disseminated amongst the responders to an emergency situation when no network connectivity is available. In such situations Delay Tolerant Networks (DTN) are used to disseminate the data by exploiting the peers' mobility in the area. However, existing DTN protection models

require recipients to be known in advance. In emergency situations the data may instead be received by unknown responders who might need it while carrying out their duties. Existing data dissemination solutions such Enterprise Rights Management (ERM) systems rely on centralized architectures where recipients must contact the authorities that can grant access to data. Such centralized solutions cannot be deployed when connectivity cannot be guaranteed. Our solution combines data protection schemes such as ERM systems with DTNs[9].

Table 1: Table of Techniques Used in Related Work

Author(s)	Year	Paper Name	Technique	Result
A. Routing Protocols in Opportunistic Network				
Anna Scaglione[1]	2006	Opportunistic Large Arrays: Cooperative Transmission in Wireless Multihop *Ad Hoc* Networks to Reach Far Distances	Opportunistic Large Array	application may arise in joint control systems and security or military scenarios
Chiara Boldrini, Marco Conti, Andrea Passarella[2]	2008	Exploiting users' social relations to forward data in opportunistic networks	context-aware approach	this approach allows automatically control congestion in opportunistic networks
J.P. Tower and T.D.C. Little[4]	2008	A Proposed Scheme for Epidemic Routing with Active Curing for Opportunistic Networks	Active Curing	We must use ER-based routing such as SERAC in a low-power radio mode for delay tolerant traffic
Gokce Gorbil, Erol Gelenbe[5]	2011	Opportunistic Communications for Emergency Support Systems	Sensor Nodes	Not secure
Zehua Wang[3]	2012	CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks	lightweight proactive source	
B. Security in Opportunistic Network				
Abdullatif Shikfa , Melek Onen , Refik Molva[7]	2010	Privacy and confidentiality in context-based and epidemic forwarding	Two pairing-based encryption,	specific use of PEKS allows intermediate nodes to securely discover partial matches between their profile
Enrico Scalavino, Giovanni Russello and Rudi Ball[9]	2010	An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios	Policy-based Authority Evaluation Scheme (PAES)	
Abdullatif Shikfa and Melek Önen and Refik Molva[8]	2012	Local key management in opportunistic networks		This also prevents Sybil attacks
B.Poonguzharselvi1 and V.Vetriselvi[6]	2012	Trust Framework for Data Forwarding in Opportunistic network Using Mobile Traces	Selection of Next Hop on trust Value	High delivery probability

III. Problems Formulation

a) Routing problems

In Opportunistic Networks (OppNets), routing is one of the main challenges. The protocols can be Epidemic Routing, PROPHET, Spray and Wait. The Epidemic routing [13] protocol is a flooding based scheme [15]. In Epidemic routing protocol each node receives a request packet and forwards the packet on its entire outgoing links except the one corresponding to the incoming link on which the packet arrives. Each request packet may reach the destination node along a different route at a different time [10][14]. The context information used in PRoPHET is the frequency of meetings between nodes, as is also seen in the MV (Meeting and Visits) and MaxProp protocols [11][12]. The design of efficient routing strategies in conventional networks is usually based on the knowledge of the available infrastructure and the network topology, whether physical or logical. Unfortunately, such knowledge is not available in such networks as the formation of data path is entirely

opportunity based. For achieving a reliable data path a trade off against the performance of the network must be met before designing the routing strategy. As the nodes are mobile and not aware about any other node until comes in his range, here finding an efficient routing protocol is difficult.

b) Privacy

The opportunistic networks present compelling challenges, especially from a security perspective. The key problem in opportunistic network is privacy. Privacy of user location, identity and the message confidentiality is the main problem. For data confidentiality we can use encryption, but we have to maintain the key of each node in the diameter of opportunistic network. And the nodes are not so big to store a number of keys and data which is carry by the nodes. Location of the user is shown to all because it can only pass the message when some other node comes in the range, hence it is easy to find that both node are at the same location and time while exchange the data. User identity is also degrading this network performance, a selfish node which is not interested to forward the message of a particular sender of his cluster or receiver of his cluster, so he drops the packet. This leads to loss of data packet.

IV. New Proposed Technique

In this research an algorithm is propose to maintain the privacy of user if user wants it. To divide the network into the clusters our research uses the concept of cluster estimation.

In this the network is initialized with the finite number of nodes. The whole network is divided into clusters. In each cluster one fixed node is defined. In fixed node database is maintained and ID of each node and password is stored. The node which wants to communicate to the other node will first communicate with the fixed node to get the virtual ID. The source node send its credentials (USER_NAME & PASSWORD) which authenticate the valid node of group and also with which node it want to communicate) to the fixed node. When fixed node verifies the credentials ,fixed node communicate with the stable node of the cluster in which destination is present and will send the virtual ID's of the source and destination , to the source node + the secure session key. Once the source node authenticates the user then stable node communicate with the stable node of destination cluster and exchange information and update their table. Now stable node of source cluster will sends a new virtual ID to the source , new ID of destination and a session key with which the source node encrypt the message. This message is now encrypt by the public key of the source node. And stable node also sends a new virtual ID to the destination, virtual id of source node and session decryption key. This message is encrypted by the public key of destination node. Source node now send message with new ID and encrypt the message with session key.

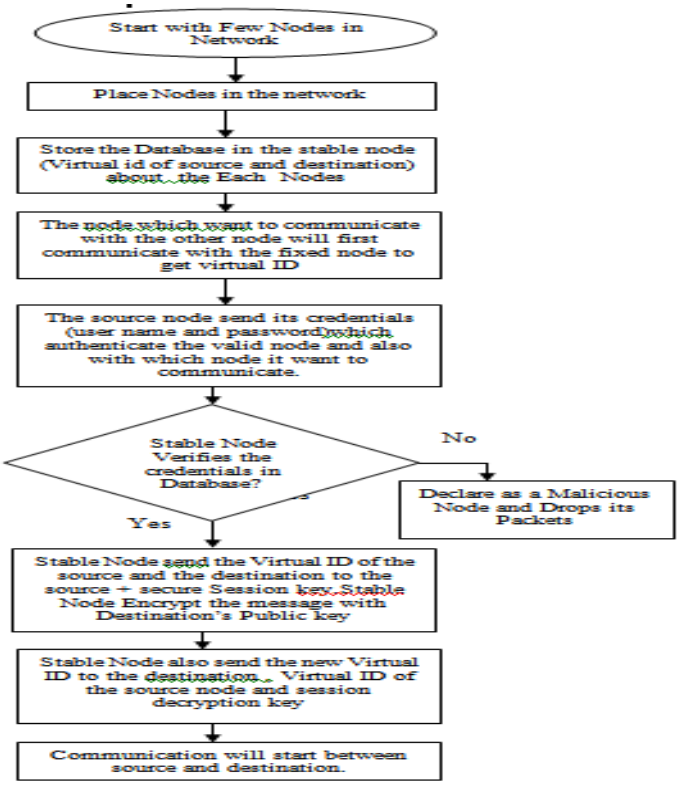

Figure 3 Flowchart of Proposed Technique

V. Results And Discussion

Results

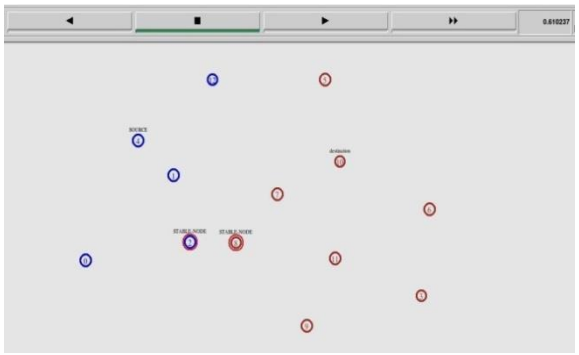

Figure 4 Proposed network designs

We consider two cluster differentiated by color and two stable node, one for each cluster shown by thick outline. Take Node4 as source node and Node10 as destination node (both are lies in different cluster). Features of the stable node is same as the other node it also transfer a message only when other nodes comes in his communication range. ID Source node request to stable node for a Virtual ID. Stable node check the table to authenticate the valid user.

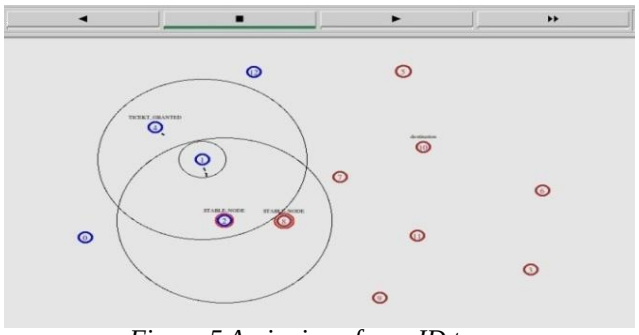

Figure 5 Assigning of new ID to source

After sharing data, stable node provides a new id to the source node. Stable node sends ticket to the source node after authentication and sharing information with the stable node of cluster in which destination is present.

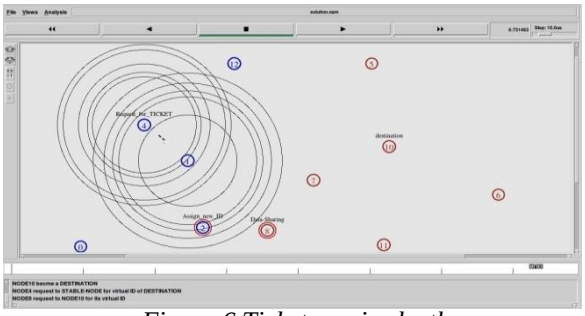

Figure 6 Ticket receive by the user

Ticket contains:

- A new virtual ID
- New destination ID
- A session key to encrypt the message.

This ticket is encrypted by the public key of source node which is present in the table of stable node. After getting the new ID, source node send the message and encrypt with the session key provides by the stable node. The message is encypted by the public key of the destination node. Destination node also gets a new ID by stable node8.

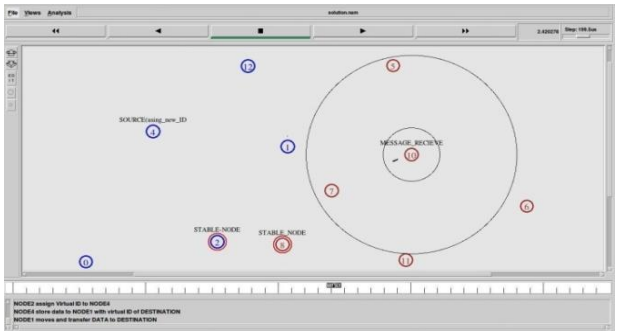

Figure 7 Message forward by intermediate node to the closer one in his range

Now the data carrying node (Node1) forward data to Node7 when appears in his communication range. Message reaches at the destination.Node7 forward the message to the destination. It will send the data to a particular destination in a very secure manner.

VI. Discussion

a) Comparison of both techniques in term of packet loss

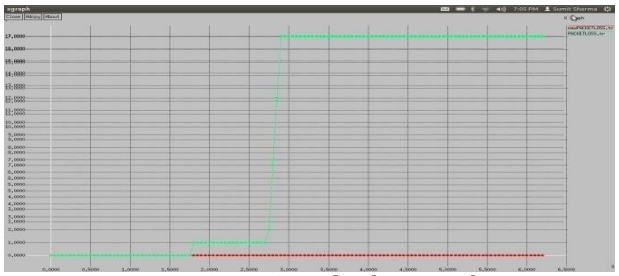

Figure 8 Packet loss graph

- Graph is plotted between the number of packet (y-axis) and the time (x-axis).
- Green line shows the packet loss by the previous method.
- Red line shows the packet loss by proposed algorithm.

b) Comparison of both methods in the form of throughput

Figure 9 Throughput graph

- Red line shows throughput by net algorithm
- Green line show throughput by previous algorithm
- Throughput is lies between 0 and 1 along y-axis
- Time along x-axis

VI. Conclusion And Future Scope

Conclusion

In this research our work finds that opportunistic network is very useful if privacy is maintained. Due to inefficient 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, this research propose 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, then he first communicate with stable node(trusted node) and get a virtual id for a period of time. Stable node act as special node, which contains information of every node of the cluster and authenticate the nodes who wishes to communicate and provide virtual id to that nodes. And also a session key is provided for encryption of message to the source and decryption key to the destination for maintaining the confidentiality of the message. The public private 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.

Future Work

In our work we purpose a technique to provide privacy to a user in opportunistic network on the basis of providing virtual 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 find a way which reduces the user work by providing some new mechanism to hide the 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]. 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.

[2]. Chiara Boldrini, Marco Conti, Andrea Passarella "Exploiting users' social relations to forward data in opportunistic Networks" 1016/j.pmcj.2008.04.003 2008 Elsevier.

[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]. J.P. Tower and T.D.C. Little "A Proposed Scheme for Epidemic Routing with Active Curing for Opportunistic Networks" In Proc. 1st IEEE Intl. Workshop on Opportunistic Networking, Okinawa, Japan, March 2008.

[5]. Gokce Gorbil, Erol Gelenbe "Opportunistic Communications for Emergency Support Systems" 1877–0509 © 2011 Published by Elsevier 10.1016/j.procs.2011.07.008.

[6]. B.Poonguzharselvi1 and V.Vetriselvi "Trust Framework for Data Forwarding in Opportunistic network Using Mobile Traces" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 6, December 2012.

[7]. Abdullatif Shikfa , Melek Önen , Refik Molva "Privacy and confidentiality in context-based and epidemic forwarding" 2010 Published by Elsevier B.V:10.1016/j.comcom.2010.04.035

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

[9]. Enrico Scalavino, Giovanni Russello and Rudi Ball "An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios" ASIACCS'10 April 13–16, 2010, Beijing, China.

[10]. Ram Ramanathan, Richard Hansen "Prioritized Epidemic Routing for Opportunistic Networks" June11, 2007, San Juan, Puerto Rico, USA.

[11]. 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.

[12]. Thrasyvoulos Spyropoulos, Konstantinos Psounis, Cauligi S. Raghavendra "Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case" IEEE/ACM Transactions on Networking, Vol. 16, No. 1, February 2008.

[13]. Mamoun Hussein Mamoun, Saud Barrak "Adaptive Priority Routing Protocol for DTN Networks" International Journal of Engineering and Technology Volume 3 No. 3, March, 2013.

[14]. A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks" Duke University, Tech. Rep. CS-2000-06, Jul. 2000.

[15]. S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," in Proc. ACM SIGCOMM, Oct. 2004.

[16]. A. Doria, M. Uden, and D. P. Pandey, Providing connectivity to the saami nomadic community, in Proceedings of the 2nd International Conference on Open Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[17]. A. Pentland, R. Fletcher, and A. A. Hasson, A road to universal broadband connectivity, in Proceedings of the 2nd International Conference on Open Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[18]. G. E. Prescott, S. A. Smith, and K. Moe, Real-time information system technology challenges for NASAs earth science enterprise, in Proceedings of The 20th IEEE Real-Time Systems Symposium, Phoenix, Arizona, Dec 1999.

[19]. P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet, in Proceedings of ACM ASPLOS, 2002.

[20]. Disruption tolerant networking, http://www.darpa.mil/ato/solicit/DTN/.

[21]. J. Ott and D. Kutscher, A disconnection-tolerant transport for drive-thru internet environments, in Proceedings of IEEE INFOCOM, 2005.

[22]. Eyuphan Bulut and Boleslaw K. Szymanski, "On Secure Multi-copy based Routing in Compromised Delay Tolerant Networks," Workshop on Privacy, Security and Trust in Mobile and Wireless systems at 20th IEEE International Conference on Computer Communications, ICCCN, Maui, Hawaii, July 31,2011.