ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Evidence forwarding of a Node in Mobile Opportunistic Social Network with proximity

[1] Dr.S.Chakaravarthi [2] D.Saranya
[1] Assistant Professor, [2] PG Scholor
[1][2] Department of Computer Science and Engineering,Velammal Engineering College,Chennai, India

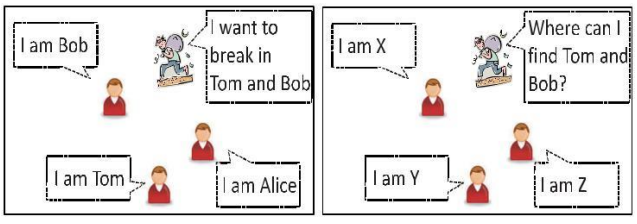
Abstract: Usually, the sending of messages or communication between the nodes are done by proximity based mobile opportunistic social network. When sending the messages from one to another there is the chance of packet loss i.e missing of information. This is usually happened by communication between the nodes are done by real id . In current method, the prevention of message or information are done by FaceChange i.e changing of real id to alias name or id. Here, we use advance method of not only preventing the information while communication but also check the trustworthy ness of the third party authority and verify whether the communication are done between the real node are alias node. This is mainly effective in group communication where we cannot check that the near by node are real node or malicious node or attacker node. Once when we come to know that the attacker node is active it gives the warning or kind of information that which node is attacker node to all other trusted node or communicating node.

Index Terms— Evidence Forwarding (EF), mobile opportunistic social network (MOSN), Third party Tursted authority (TTA).

I. INTRODUCTION

In mobile opportunistic social networks have attracted much attention due to the increasing popularity of mobile devices. e.g., smartphones and tablets. In MOSNs, mobile devices carried by people communicate with each other directly without the support of infrastructures. when they Meet within the communication range of each other , it may face a serious challenges due to various types of attacks Here, we see about prevention of nodes from the attack of malicious node and trusted authority. Even though the transmission are done in effective and efficient manner there is the chance of packet loss which cause the loss of information while transfer of messages.

A communication model can be utilized to support various applications without infrastructures, such as packet routing between mobile nodes , encountering based social community/relationship detection and distributed file sharing in a community. to know whom they have met to identify proximity based social community/relationships.



(a) (b)

FIG 1.1 (a) Possible privacy issue. (b) Solution: neighbor Anonymity.

2.LITERTURE SURVEY

2.1 A Complex Network Analysis of Human Mobility (by : Theus hossmen –switzerland ,Thrasyvoulous Spyropoulus – France , Franck Legendre – switzerland) (23 June 2011 /IEEE_Xplore) Opportunistic networks use human mobility and consequent wireless contacts between mobile devices, to disseminate data in a peer-to-peer manner with some algorithm and protocol to understand the statistics of contacts. The contact analysis on statistics with pair-wise properties which has structural properties. Methodology to represent a mobility scenario as a weighted contact graph, where tie strength represents how long and often a pair of nodes is in contact. This allows us to analysis the structure of a scenario using tools from complex network analysis and graph theory with the global distribution of intera -community structure.

2.2 Poster: Probabilistic Routing in Intermittently ConnectedNetworks
(by : Anders Lindgren – Sweden , Avri Doria – sweden , Olov Schelen – sweden)(Volume 7 Issue 3, July 2003/ ACM SIGCOMM Computer Communication)

The problem of routing in intermittently connected networks causes serious impact. In such networks there is no guarantee that a fully connected path between source and destination exist at any time.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Rendering traditional routing protocols unable to deliver messages between hosts nodes.A probabilistic routing protocol for such networks are provided which show the efficient performance.

2.3 *DTN Routing as a Resource Allocation Problem* (by: Aruna Balasubramanian, Brian Neil Levine and Arun Venkataramani Department of Computer Science, University of Massachusetts Amherst, MA, USA)(Volume 37 Issue 4, October 2007)

Many DTN routing protocols use a variety of mechanisms, including discovering the meeting probabilities among nodes, packet replication, and network coding.The primary focus of these mechanisms is to increase the likelihood of finding a path with limited information with the approaches having maximum or average delivery delay.RAPID an intentional DTN routing protocol that can optimize a specific routing metric such as worst-case delivery delay or the fraction of packets that are delivered within a deadline.RAPID rigorously through a prototype deployed over a vehicular DTN test bed of 40 buses and simulations based on real traces which has 10% outperformance in efficiency.

2.4 *Routing in a Delay Tolerant Network* (by : Sushant Jain –wahington, Kelvin Fall –Berkeley, Rabin Patra –Berkeley)(Volume 34 Issue 4, October 2004/ ACM SIGCOMM Computer Communication)

The delay-tolerant networking routing problem, where messages are to be moved end-to-end across a connectivity graph that is time-varying but whose dynamics may be known in advance. The added constraints of finite buffers at each node and the general property that no contemporaneous end-to-end path may ever exist.A framework for evaluating routing algorithms which develop several algorithms and use simulations to compare their performance with respect to the amount of knowledge.With the additional global knowledge , the efficient algorithm is build to rectify the routing problem in DTNs.

2.5 *A Method for Obtaining Digital Signatures and Public-Key-Cryptosystems*
(by : R.L. Rivest, A. Shamir, and L. Adleman)(Volume 21 Issue 2, Feb. 2000 / Communications of the ACM)

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key . Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only can decipher the message using corresponding decryption key. A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature.

2.6 *An Efficient and Secure ID Based Group Signature Scheme from Bilinear Pairings* (by -:Pankaj Sarde _- Raipur , Amitabh Banerjee – Raipur) (May/Jun 2015 / ProQuest)

An efficient and secure identity based group signature scheme from bilinear pairings. Group signature allows group member to sign arbitrary number of messages on behalf of the group without revealing their identity.The group manger holding a tracing key can reveal the identities of the signer from the signature. On the Computation Diffie-Hellman Problem (CDHP) assumption and bilinear pairings, the size of the group public key and length of the signature are independent on the numbers of the group members.

2.7 *Safety Challenges and Solutions in Mobile Social-Networks*
(by : Yashar Najaflou, Behrouz Jedari, Feng Xia - senior member of IEEE)(21 october 2013 /IEEE Xplore)

Mobile social networks (MSNs) are specific types of social media taking advantage of the characteristics of both social networks and opportunistic networks (OppNets), MSNs are capable of providing an efficient and effective mobile environment for users to access, share, and distribute data. To provide a clear categorization on safety challenges and a deep exploration over some recent solutions in MSNs which is the lack in previous scenario.This work narrows the safety challenges and solution techniques down from OppNets and delay-tolerant networks to MSNs with the hope of covering all the work proposed around security, privacy, and trust in MSNs.

2.8 *Dynamic Social Feature-based Diffusion in Mobile-Social-Networks*
(by : Xiao Chen , Kaiqi Xiong –San Francisco) (07 April 2016/IEEE Xplore)

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

The diffusion minimization problem whose goal is to select an optimal set of initial nodes to disseminate the information to the whole network as quickly as possible.

By taking advantage of node social features in MSNs, dynamic social features to capture nodes dynamic contact behaviour and use social similarity metrics to measure their social closeness.The community concept in social networks to reduce the complexity of the diffusion minimization problem. Diffusion node selection algorithms based on these new features to minimize the diffusion times with the result of algorithms having lower diffusion times than the existing ones.

2.9 *SMART: Lightweight Distributed Social Map Based Routing in Delay Tolerant Networks*
(by : Kang Chen and Haiying Shen- Clemson) (14 February 2013/ IEEE Xplore)

when two nodes meet, they have to exchange the delivery probabilities to the destinations of all packets in the two nodes, which incurs high resource consumption.
A lightweight distributed Social MAP based Routing algorithm in delay Tolerant networks (SMART) where each node builds its own social map consisting of nodes it has met and their frequently encountered nodes in a distributed manner. The weight of each link to reflect the packet delivery probability between the two nodes where social map enables more accurate forwarder selection through a broader view. Nodes exchange due to social map stability, which reduces resource consumption where Trace-driven experiments and tests on the GENI ORBIT test bed demonstrate the high efficiency of SMART in comparison with previous algorithms.

2.10 *Impact of Human Mobility on Opportunistic Forwarding-Algorithms*
(by : Augustin Chaintreau, Pan Hui, Jon Crowcroft, Fellow, IEEE) (30 April 2007/IEEE Xplore)

Data transfer opportunities between wireless devices that has the distribution of the inter contact time may be well approximated by a power law over the range.The newly uncovered characteristic of human mobility impacts one class of forwarding algorithms previously proposed which is a simplified model based on the renewal theory to study how the parameters of the distribution impact the performance in terms of the delivery delay of these algorithms.The design of well-founded opportunistic forwarding algorithms in the context of human-carried devices.

3. FACECHANGE

when nodes meet, they simply communicate with their real IDs, which leads to privacy and security concerns. In current MOSN applications, nodes can collect real ID based encountering information easily since neighbor nodes communicate with real IDs directly. However, when using real IDs directly, the disclosure of node ID to neighbor nodes would create privacy and security concerns. For example, a malicious node can first know the IDs of nodes with specific interests when neighbor nodes communicate with real IDs, a malicious node can easily identify attack targets from neighbors and launch attacks to degrade the system performance or steal important documents. Further, without protection, malicious nodes can also easily sense the encountering between nodes for attacks.
The prevents nodes from collecting real ID-based encountering information, which is needed to support MOSN services. Therefore, in this paper, we propose Face Change that can support both anonym zing real IDs among neighbor nodes and collecting real ID-based encountering information. For node anonymity, two encountering nodes communicate anonymously. When the two nodes disconnect with each other, then each node forwards an encountering evidence to the node to enable encountering information collection.

3.1 PROBLEM IN FACECHANCES:

(i) The security of the encountering evidence needs to be ensured.
(i) An encountering evidence can only be accessed by its creator and recipient and cannot be forged.
(iii) An encountering evidence needs to be successful delivered to its recipient even when the real ID of the recipient node is unknown due to neighbour node anonymity.
(iv) When creating an encountering evidence, a node can control what contents to be included based on its trust on the encountering node.
(v) The calculation of the trust should be privacy-preserving method.
(vi) Attacker easily get the user id to hack account or leak the documents.
(vii) In addition, it is still can not limit or control various attack behaviors.
(viii) It doesn't check the trustworthiness of the mutually trusted authority.
(ix) It doesn't validate the neighboring user nodes.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

4 TECHNIQUE USED

The real ID are changed to the alias name by(i) FaceChanges, which is given by third party authority on(ii) (MONS).After the exchange of information is done , each(iii) node create Encountering evidence of information. The(iv) encountering evidence of information are shared between the mutually trusted node to verify weather the trusted authority(TA) is trustworthiness. This encountering evidence information exchange also helps to validate that the user node is original node or malicious node. The encountering evidence of information with time, real ID, alias name or alias ID in the encrypted form along with the signature. This provide the confidential way communication between the neighboring nodes. The encountering evidence of envelope shared between the nodes after the communication helps to verify the trustworthiness of the trusted authority. The signature send by the TA, helps to verify the valid user or malicious node.Here, while communication are done i.e is while chatting the messages are send from one to another in encrypted form and the messages are received at the another end by decrypting form which is done by RSA algorithm and signature are used as private key while decrypting. The request are done to connect one another where the H-MAC algorithm for security and authentication are used and ID-BASED algorithm are used to change the real id or name of the node with more secure way of bilinear paring .

Fig 4.1 identification of near by node

5 MODULES

Network Formation
Neighbor node calculation
Data communication
Evidence forwarding

(i) Network Formation:

First we can create a Trusted Authority and then create network node assume the communication range of a node is finite. By providing distance and range ie Coverage of an particular node. Node in the network would contain unique real ID and port number for communicate with other node. Node generate it own alias name or alias id for security purpose. Node can send the data to the other node directly when the destination node is willing to communicate with that node then only the node can send data or chat with the node .

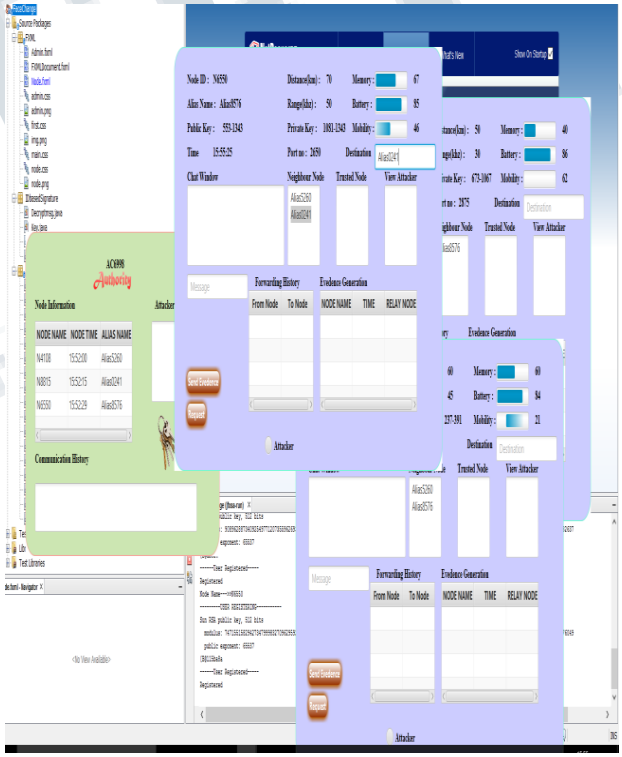


Fig 5.1 network formation

Create a Trusted Authority and then create network node assume the communication range of a node is finite. Node in the network would contain unique real ID and port number for communicate with other node. Node generate it own alias name or alias id for security

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

purpose and can send the data to the other node directly.The node enter to the network each node have their own and unique digital signature that would generated based on their real id.The unique signature is used , in order to determine the valid user in the network.

(ii) *Neighbour node calculation*

Node need to find their nearby neighbor before starting any communication. Neighbor is calculated based on the coverage of each node , when the node comes the coverage range of the other node then the two node will consider as the neighbor node . neighbor node also know by alias name only. Node can be know in the network by their alias name to maintain the node privacy. Node can send the request to other node only when the other node are in the coverage range And for that purpose node need to find their nearby neighbor before starting any communication. Neighbor is calculated based on the coverage of each node .when the node comes the coverage range of the other node then the two node will consider as the neighbor node .Then the neighbor node also know by alias name only. The calculation are done to find the near by node with distance and range value . This helps to find the near by neighbor node with some values of alias name or alias id.

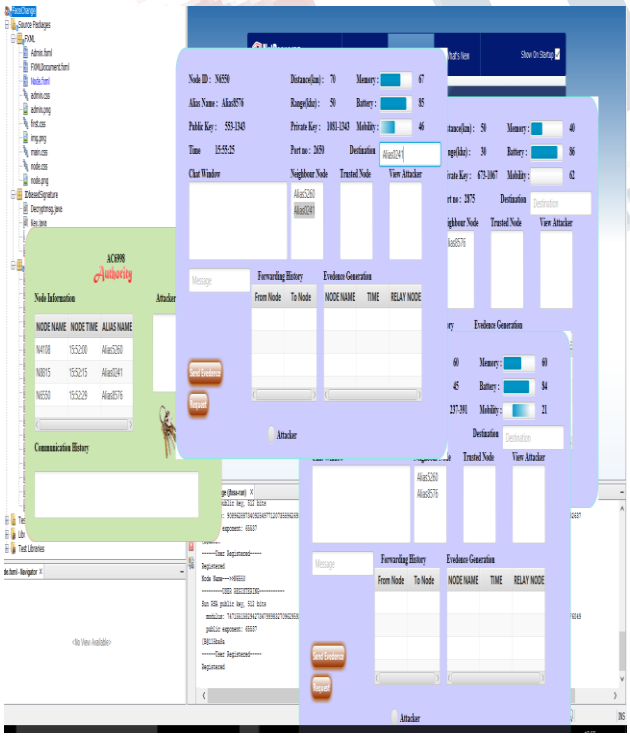


Fig 5.2 neighbour calculation

(iii) Data Communication

Once the node enter in the network node will generate its alias name or alias id each node in the network would hide their real Id and shown only the alias name to all the near by node , Only the trusted authority know the real id as well as the alias name of an each node and trusted authority would maintain evidence of data communication between nodes.Node first send the chat request to any one of the neighbor node when the destination node accept the request the both the will chat with each other Chatting or communication between two node is provided by the alias name only. Once the disconnect with each other node the two node will exchange the envelop with each other. The node enter in the network node will generate its alias name or alias id each node. Only the trusted authority know the real id as well as the alias name of an each node. Trusted authority would maintain evidence of data communication between nodes.Node first send the chat request to any one of the neighbor node when the destination node accept the request.

The both node chat with each other communicate between two node is provided by the alias name only.Once the disconnect with each other node the two node will exchange the envelop with each other.

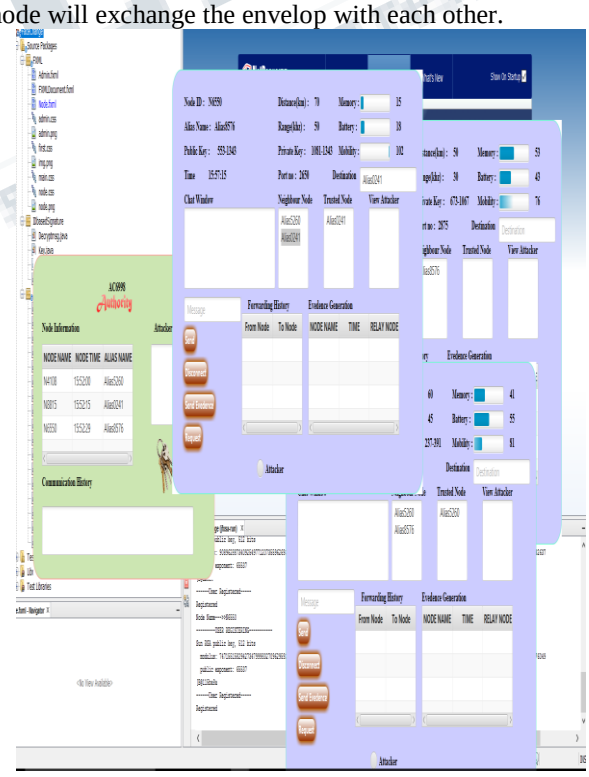


Fig 5.3.1 data communication

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

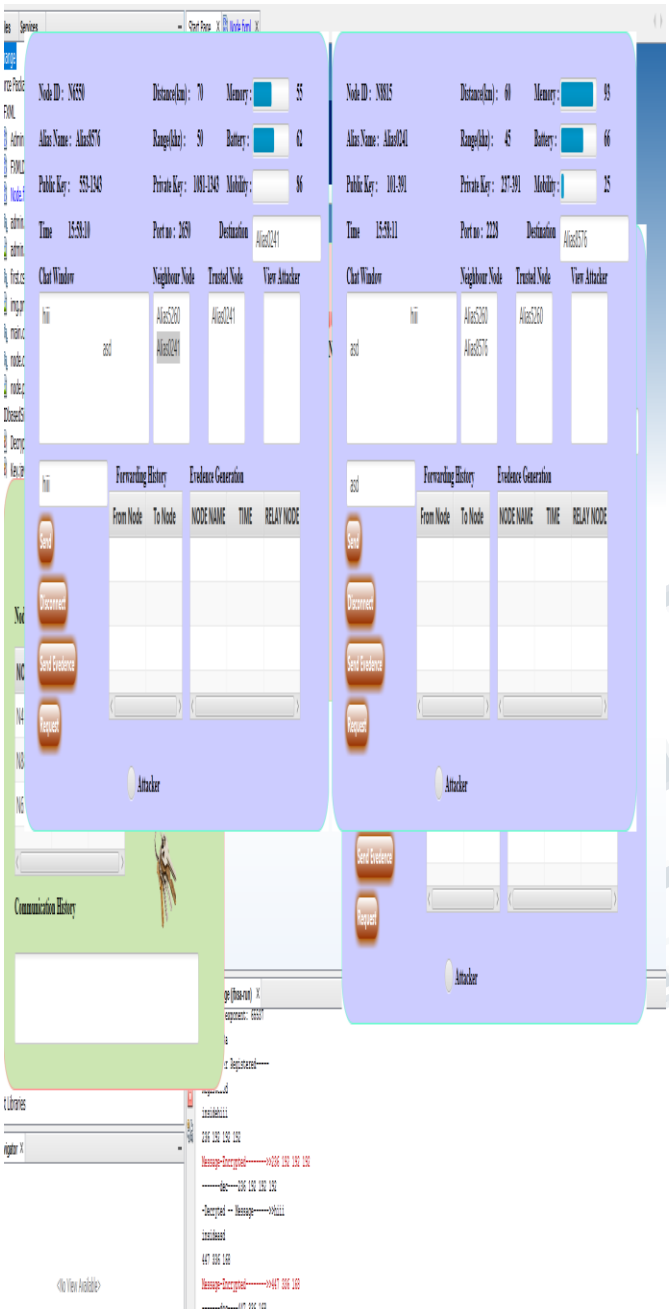


Fig 5.3.2 data communication

(iv) Evidence forwarding:

In each system, a node is uniquely labeled by an unchanging ID (defined real ID), which is obtained from the trust authority (TA), for the corresponding service. Since those services are built upon node encountering, nodes need to collect real ID based encountering information. the design of FaceChange. When two nodes meet, they communicate anonymously. However, each of them creates an encountering evidence that contains their real IDs. When the destination node accept the request the both the will chat with each other Chatting or communication between two node is provided by the alias name only. Once the disconnect with each other node the two node will exchange the envelop with each other. The envelop contain the real id of the particular node . each node need to forward envelop to the relay node that provided by trusted authority and maintain the evidence.

The forwarding envelope has real name, alias, name and time which is used to cross verify the node transmission. Once the communication is done between the node , it disconnect with the third party authority and each node create its own envelope . this envelope is used to verify the trustworthy ness and also which node is real node and which node is malicious node. To find out or verifying the communication we maintain the authority section where we have one column of alias name, real name, time and another column of attacker node, and communication history and key symbol.

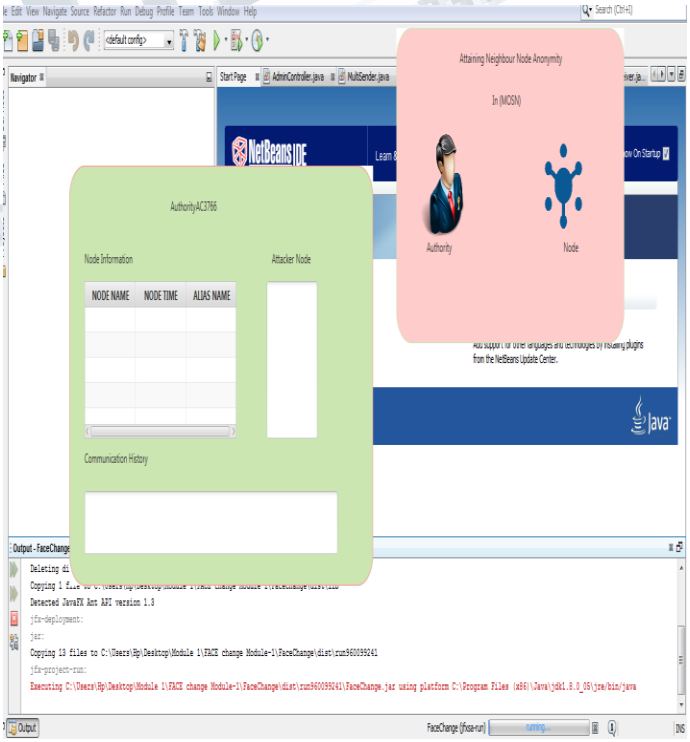


Fig 5.4 authority and node

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

This verification can be done in three ways.

1.By maintaining the history.
2.Packet loss
3.Attacker activation

1. By Maintaining The History

Here , when the distance and the range of the node are given to find out the near by neighboring node. The request is given to the near by neighboring node to start the data communication between them and this is done by the key user in the Authority section. Once the request is accepted by the near by node , the chat application start to work where the exchanging of information is done between them. Once the evidence send is used , it ask for the content, forwarding, near by node and the main node id. The node id should be given. Once these are done , the history is maintaines in authority section saying the commucation between the node is happened.

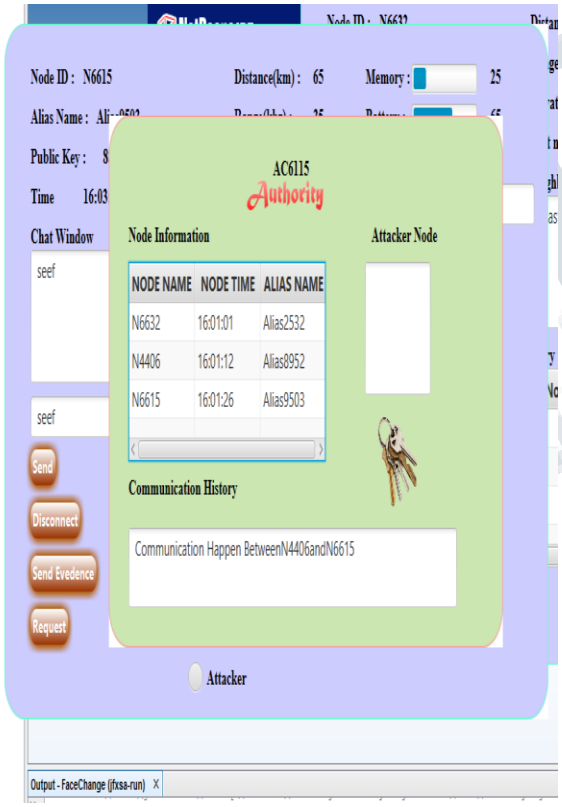


Fig 5.4.1 communication history

2.Packet loss

Here , when the distance and the range of the node are given to find out the near by neighboring node. The request is given to the near by neighboring node to start the data communication between them and this is done by the key user in the Authority section. Once the request is accepted by the nearby node , the chat application start to work where the exchanging of information is done between them. Once the evidence send is used , it ask for the content, forwarding, nearby node and the main node id. Once the forwarding is not given that automatically says that there is packet loss which mean there is missing of information . this missing of packet leads the accepted user to be the attacker which is specified in the Authority section. Them it ask for the node id , when it is specified, it gives the communication history saying that there is the attacker between but the chat was done between the connected node.

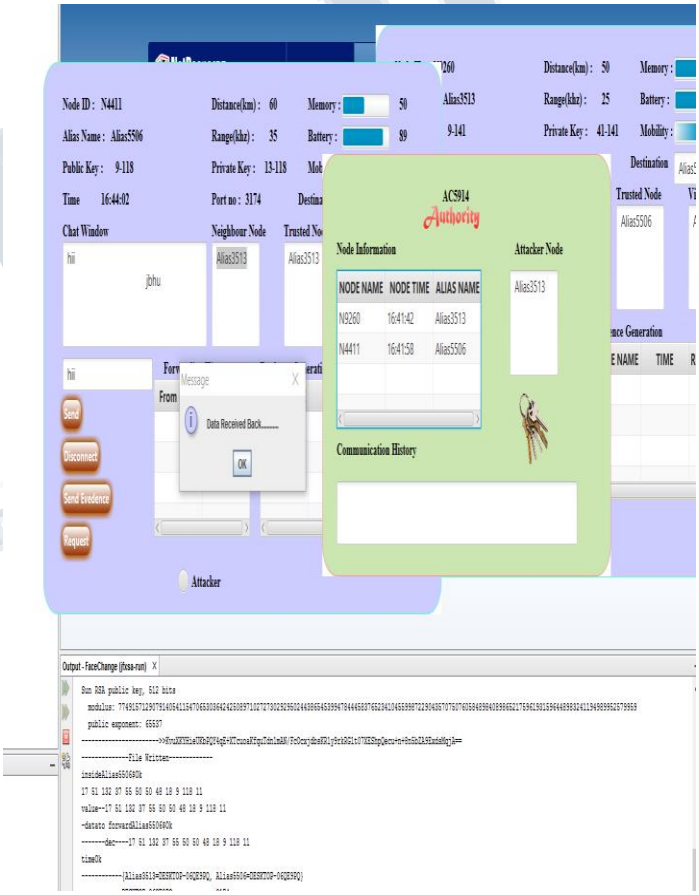


Fig 5.4.2 packet loss

3.Attacker Activation

Here , when the distance and the range of the node are given to find out the near by neighboring node. The request is given to the near by neighboring node to start the data communication between them and this is done by the key user in the Authority section. Once the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

request is accepted by the near by node , the chat application start to work where the exchanging of information is done between them. When the attacker node is activated and the evidence sending node act as the trusted node then, when forwarding the evidence it says as the packet loss and specify as that destination node as the attacker node in the Authority section.

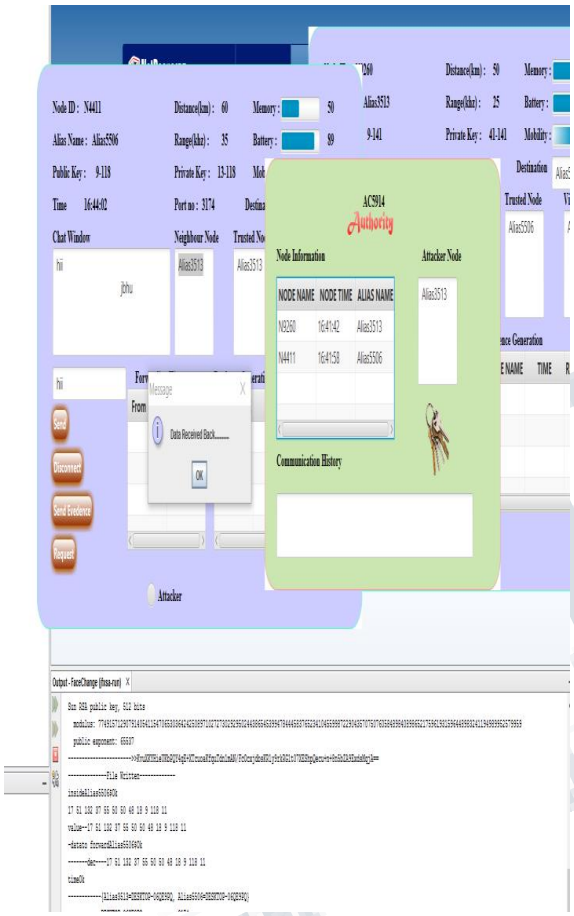


Fig 5.4.3 attacker activation

6. CONCLUSION

The communication between the neighboring nodes with the changes in pseudonyms and parameters to hide its real ID from the malicious node of attacker provide the security and integrity.The evidence of envelope which has the time, real ID, alias name provides the validity of the user nodes.The encountering evidence of information shared between the neighboring nodes after the communication provides the trustworthiness of the mutually trusted authority.This exchange of encountering evidence of information provide the surety about both the neighboring nodes of the user and trusted authority.

11.REFERENCE

[1] X. Zhang and G. Cao, "Transient community detection and its application to data forwarding in delay tolerant networks," in Proc. IEEE ICNP, Oct. 2013, pp. 1–10.

[2] S. Zakhary and M. Radenkovic, "Utilizing social links for location privacy in opportunistic delay-tolerant networks," in Proc. IEEE ICC, Jan. 2012, pp. 1059–1063.

[3] X. Lu, P. Hui, D. Towsley, J. Pu, and X. Zhang, "Anti-localization anonymous routing for Delay Tolerant network," Comput. Netw., vol. 54, no. 11, pp. 1899–1910, 2010.

[4] Q. Li and G. Cao, "Efficient and privacy-preserving data aggregation in mobile sensing," in Proc. IEEE ICNP, Nov. 2012, pp. 1–10.

[5] X. Wang et al., "Stamp: Ad hoc spatial-temporal provenance assurance for mobile users," in Proc. IEEE ICNP, Oct. 2013, pp. 1–10.

[6] P. Aditya et al., "Encore: Private, context-based communication for mobile social apps," in Proc. MobiSys, 2014, pp. 135–148.

[7] J. Manweiler, R. Scudellari, and L. P. Cox, "Smile: Encounterbased trust for mobile social services," in Proc. CCS, 2009, pp. 246–255.

[8] L. P. Cox, A. Dalton, and V. Marupadi, "Smokescreen: Flexible privacy controls for presence-sharing," in Proc. MobiSys, 2007, pp. 233–245.

[9] M. Lentz et al.,"Sddr: Light-weight, secure mobile encounters," in Proc. 23rd USENIX Secur. Symp. (USENIX Secur.), 2014, pp. 925–940.

[10] W. Gao and Q. Li, "Wakeup scheduling for energy-efficient communication in opportunistic mobile networks," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2058–2066.

[11] B. B. Chen and M. C. Chan, "MobiCent: A credit-based incentive system for disruption tolerant network," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[12] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," IEEE Trans. Wireless Commun., vol. 9, no. 4, pp. 1483–1493, Apr. 2010.

[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[14] F. Miller, Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams. New York, NY, USA: Cornwell, 1882.

[15] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Germany: Springer, 2010.

[15] Ubuntu Network Configuration, accessed on Oct. 10, 2015. [Onilne]. Available: https://help.ubuntu.com/community/NetworkConfigurationCommandLine/Automatic

[16] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in Proc. PKC, 2004, pp. 277–290.

[17] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," ACM SIGMOBILE Mobile Comput. Commun. Rev., vol. 7, no. 3, pp. 19–20, 2003. [42] J. Golbeck, "Trust and nuanced profile similarity in online social networks," ACM Trans. Web, vol. 3, no. 4, 2009, Art. no. 12.

[18] R. C. Merkle, "Secure communications over insecure channels," Commun. ACM, vol. 21, no. 4, pp. 294–299, 1978. [19] N. Eagle, A. Pentland, and D. Lazer, "Inferring friendship network structure by using mobile phone data," Proc. Nat. Acad. Sci., vol. 106, no. 36, pp. 15274–15278, 2009.

[20] A. Chaintreau et al., "Impact of human mobility on opportunistic forwarding algorithms," IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620, 2007. [46] K. Chen and H. Shen, "Fine-grained encountering information collection under neighbor anonymity in mobile opportunistic social networks," in Proc. IEEE ICNP, Nov. 2015, pp. 179–188.