ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

# Trust Preservation in Opportunistic Networks

Anant Khot[1], Prof. Vishal Mogal[2]

M.E., Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India[1]

Assistant Professor, Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India[2]

**ABSTRACT**: Opportunistic networks or Delay Tolerant Networks (DTNs) becoming an active research area in wireless communication. Opportunistic networks are characterized by the outsized end to end communication latency and non-availability of instantaneous end to end path from a source to its destination. Preserving trust and security in such opportunistic networks are the most important tasks. Suitable settings are needed to improve routing performance and minimize the trust bias in such wireless networks. In this paper, the security preferences of opportunistic network are considered. Moreover, by using suitable mechanisms few ways for misbehaviour detection of routing and dropped packets recognition are exposed. The remark is also made with the overall analysis.

**KEYWORDS**: Misbehavior Detection, Opportunistic Networks, Security, Social selfishness, Trust management.

## I. INTRODUCTION

Wireless communication networks offers wide range of advantages over wired networks. The Delay Tolerant Network (DTN) is a type of network in which communication takes place without network infrastructure. Opportunistic networks are class of DTN where mobile users are in large scale and it provides them the facility to exchange the content via short range communication whenever they encounter each other. In opportunistic networks mobile nodes do undergo from frequent discontinuations, asymmetric links and continuously altering network topology. Opportunistic network supports Store, carry and forward mechanism. It supports persistent content storing and forwarding through the number of intermediate nodes as shown in Fig1.

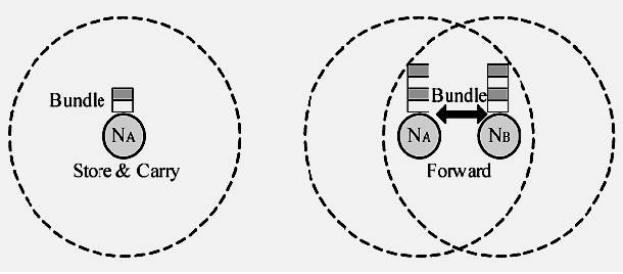


**Fig1.** Bundle store-carry- forward in DTN

## II. RELATED WORK

Ing-Ray Chen et al have suggested a dynamic trust based routing protocol [1] by validating direct trust and indirect trust among nodes of opportunistic network. This validation is done by evaluating the trustworthy properties (such as healthiness, unselfishness, connectivity and energy) of every encountering node. Healthiness, unselfishness and energy are considered to get maximum message delivery ratio, and connectivity to minimize message delay. In this protocol the level of trust of every node is considered in [0,1], where 0 indicates complete distrust and 1 represent complete trust. This way trust value of one node is evaluated by another encountering node and that computed trust is weighted as averaging trust of these properties. Authors have used healthiness and unselfishness as two social trust metrics to deal with both socially selfish and malicious nodes. It can be helpful for message forwarding by determining the QoS and trust related properties of every node in opportunistic network. A Stochastic Petri Net technique (SPN) [12] is used

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

to implement a probability model for Dynamic Trust Management Protocol [1]. It consists of four places, such as energy, location, maliciousness and selfishness. Here energy is indicating the amount of energy left in the node in integer, location indicates the location of the node, maliciousness represents a binary variable with 1 indicating the node is malicious and 0 indicating non-malicious. Selfishness is also a binary variable; in case of 1 it indicates that the node is socially selfish and 0 otherwise. From such assumptions a node may forward a packet only if the node (source, intermediate or the destination) is exist in its friend list. The crucial role of the SPN model is to return status of a node in terms of its healthiness, unselfishness, connectivity, and energy. The obtained status of node helps to validate trust of protocol.

An Iterative Trust and Reputation Mechanism (ITRM) can be helpful in managing the reputation and trust in DTNs [2]. ITRM is iterative scheme beneficial for determining the service quality of every peer and detecting the presence of malicious nodes within the DTNs using graph based iterative algorithm. ITRM uses two kinds of sets such as set of service providers (SPs) and set of service consumers (SCs). After each communication among SPs and SCs, SCs acknowledges to SPs in the form of ratings about its service. Authors have summarized few trust related major attacks that can occur frequently in opportunistic networks, which are as follows.

- **Self-promoting attacks:** It can promote its importance (by providing good recommendations for itself) so as to attract packets routing through it (and being dropped).
- **Bad-mouthing attacks:** It can decay the way of content routing through good nodes by promoting bad recommendations against good nodes.
- **Ballot stuffing:** It can increases the content routing through bad nodes by providing good recommendations for them. When a node encounter with another node then they can exchange encounter history so as to prevent attacks like black hole attack.

In this iterative adversary detection algorithm authors have picked an arbitrary node in the network. That node is considered as a judge. This judge node can make its own rating of another nodes of network by receiving feedbacks and collecting them. Each judge node has its rating table to store the ratings of the network nodes obtained from feedback. Authors have presented these ratings or feedbacks in 0 or 1 [2]; it denotes the binary reputation values. So a node with 0 reputation value indicates as a malicious node. In this case, this iterative reputation scheme can become a detection scheme. Mieso K. Denko et al have suggested a management scheme of Trust management in ubiquitous computing: A Bayesian approach is support to a node to evaluate the trustworthiness of another node, it encounters with, while dealing with the maliciousness behaviors in the network [3]. The Bayes theorem is based on probability theory, used to design a trustful model for opportunistic networks. Still to distinguish between malicious and non-malicious nodes is quite complex task due to lack of trust. The trust in a device can be determined by evaluating the direct trust computation and indirect trust computation. This is done by accounting the previous history and recommendations from other devices relating to its services. Bayesian approach can be used for allowing the devices to detect maliciousness of device interacting with it, behavior expectations of dynamic change in malicious devices, protection against false recommendation attacks and its impacts on devices.

Q. Li et al. has proposed a Social Selfishness Aware Routing (SSAR) algorithm to allow user selfishness and provide better routing performance in an efficient way [8]. SSAR helps to select an accelerating node; it considers users willingness to forward and their encountering situations, subsequent in a better forwarding scheme. For maintaining a better forwarding scheme SSAR assigns wealth. This wealth can involve buffers and bandwidth based on packet priority. It is related to the social relationship among nodes and provides heuristic solution for content forwarding [8].

Alessandro Mei et al have proposed two forwarding protocols for mobile wireless networks of selfish nodes [7]. Those two protocols are Give2Get Epidemic Forwarding and Give2Get Delegation Forwarding. Authors have assumed that all nodes in the network are selfish and may not deviate from protocol. By using these two protocols they have tried to minimize replicas in the network and forward the message fast. G2G Epidemic forwarding protocol consists of three crucial steps such as message generation, relay, and test [7]. Authors have used public key cryptography for message security and provided a facility to hide the sender of message for every possible relay except the destination. G2G Epidemic forwarding protocol may prevent dropping of message by those who receive the message. G2G

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Delegation Forwarding minimizes the number of replicas so it can significantly reduce the cost of forwarding, without reducing the success rate and delay. For G2G Delegation forwarding the Delegation Destination Frequency and Delegation Destination Last Contact is considered. G2G Delegation Forwarding consists of four steps: Message generation, relay, test by the sender, and test by the destination. So these two protocols can be used for message forwarding by minimizing some amount of replicas in the network [7].

An alternate to Epidemic for improving routing performance Lindgren, et al has proposed a framework for probabilistic routing in intermittently connected networks [10]. It considers delivery predictability as a probabilistic metric for probabilistic routing in opportunistic networks. Probabilistic Routing Protocol using History of Encounters and Transitivity (PROPHET) is a non-trusted routing protocol [10]. PROPHET uses metric that is Delivery predictability for forwarding packets to next node. Whenever two nodes encounters then they exchange histories and delivery predictability information and this information can be used for further routing. As PROPHET provides better routing for content delivery but it may not be a trustworthy protocol for content forwarding in the opportunistic networks. Trustless opportunistic network leverages to content loss, delay, and content overheads.

Vahdat and Becker presented a routing protocol for intermittently connected networks called Epidemic Routing [11]. It is based on the epidemic routing algorithm. It generates pair-wise information of messages between the nodes as they encounters with each other to deliver the messages to their destination. An index of these messages, called a summary vector, is kept by the nodes, and when two nodes meet they exchange summary vectors [11]. Vahdat and Becker presented that by choosing an appropriate maximum hop count, rather high delivery rates can be achieved, while the required amount of resources can be kept at an acceptable level in the scenarios used in their evaluation [11]. So Epidemic Routing protocol can be used to maximize the message delivery rate, minimize message latency, and minimize the total resources consumed in message delivery.

## III. PROPOSED ALGORITHM

### A. *DESIGN CONSIDERATIONS:*

Opportunistic network allows its mobile users to form a social network for instantaneous communication. In such social or opportunistic network any node can misbehave or act as a selfish node while forwarding contents. In opportunistic networks nodes can act with different kinds of behaviors as described below,

- **Individual Selfishness:** In this category node can forward only those messages which are made by it and drop messages from other node.
- **Social Selfishness:** Socially selfish nodes are always willing to support others with whom they have social bonding and takes undue advantage out of it. Support of such nodes can be different as per the bonding. It can be considered as interpersonal bonding that may be strong or weak. As per the bonding (strong or weak) selfish users can provide services. For strong bonding they provide good service than weaker bonding.
- **Malicious nodes:** Malicious nodes may exist in opportunistic network, they may attack to weaken the connectivity among the nodes of network. So content delivery cannot be assured if such kind of nodes exist in network and resending of content is not good solution.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

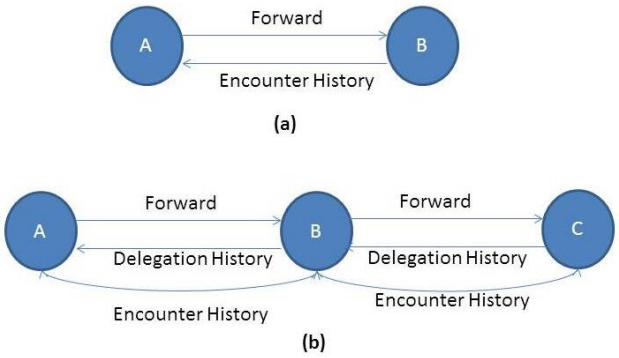


**Fig2.** System Design

Fig2. represents two different scenarios (a) Direct trust (b) Indirect trust. In (a) when node A forwarding content to node B then A and B both exchange encounter as well as delegation histories and accordingly A decide whether B is suitable node or not. In this case A act as Trustor and B as Trustee. In (b) A forwards packets to B, then gets the delegation history back. B holds the packet and then encounters C. C gets the encounter history about B. Every node in opportunistic network records and exchange three important things such as Encounter history, delegation history and forward history. By using these three kinds of information Trustor can evaluates nodes behavior for selecting next hop to forward contents. We can get complete workow of system design in Fig2 From Fig2 Trustor can assess direct trust and indirect trust by using trust property X at time (t+dt) [1].

## IV.PSEUDO CODE

Algorithm: **Trustworthy routing in DTN (Ni, TI, Hi)**
Input: Ni=Number of nodes (i, m, j),
TI= Trust information,
Hi= History,
Output: Trust value of node j = Tij(t + dt)

Step1. Node i encounters node m
Step2. Node i and m exchange TI, Hi
Step3. Node i evaluates trust property X of node j
If m=j then,
Use direct trust observation to update
Tij direct X (t + dt)
Else
Use indirect trust observation recommendations to update
Tij indirect X (t + dt)
Step4. Combine both direct and indirect trust to compute Tij X (t + dt)
Step5. Compute overall trust by combining four components Tij (t + dt)
Step6. Use computed trust value of Tij (t + dt) for selecting next message carrier
Setp7. End.

## V. IMPLEMENTATION DETAILS AND RESULTS

We used Eclipse as an implementation tool and Java as a programming language for designing and validating the trust based mechanism for misbehavior detection of node in the Opportunistic Networking Environment. Based on various movement models, the specific scenarios are created. We are used the routing protocols available for opportunistic network such as Epidemic, PRoPHET. The routing function is implemented by routing modules. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

modules decide which message to forward over existing contacts. The event generators generate the messages. The messages are unicast, having single source and single destination. Simulation reports such as encounter history, Delegation history and forward history, etc. are generated through report generator. Each node has interface, persistent storage, movement, energy consumption and message routing. The nodes move according to movement models.

A. ***NETWORK MODEL***

The opportunistic network environment is created with the opportunistic nodes. It contains two groups of nodes as P and C. The routing setting used as described below:
Interface= Bluetooth
Transmit Speed= 250k
Transmit Range= 100 M
Movement Model= Shortest Path Map Based Movement
Router= Epidemic
Buffer Size= 5M
Experimented on Intel i3 M380 2.52 GHz processor and 3.00 GB RAM.

***B. RESULT TABLES***

In trust validation process, we defining three kinds of data forwarding evidences or reports that could be used to judge whether a node is a malicious one or not:

- **Encounter History:** In this type of history, whenever two nodes meet each other, the signature is generated using the nodes and timestamp. The algorithm used for signature is MD5. As shown in figure 4, when the nodes P2 and shown in Fig.3, when the nodes P2 and C7 meet each other; to show the evidence of their meeting the signature is generated. In this way the encounter history is created for all contacted nodes. This encounter history is used by trustor node that is having trust authority at the time of misbehavior detection.

| Encounter History | | |
|---|---|---|
| ContactedNodes | | Signature |
| P2 | C7 | fed056d6d1700ab126a6d5a5db43c93a |
| P2 | C5 | cec5f9411e3fec2f122ddfc1bfab97b9 |
| C7 | C5 | b4a146cb7db2f562fa98123238a607c7 |
| C6 | C5 | b38d9c8d82fdf5303862a9b6416ee3ee |
| P3 | P1 | 6a8f5d412812153f9a097b236bb91365 |
| P0 | C5 | efc4c1a6e8d410fa2f5075b310e0644c |

**Fig.3** Encounter History

- **Delegation History:** When one node forwards the packet to next node then the next node gives the history back to its source node. As shown in Fig.4, when the node P2 forwards the packet to P1 then node P2 gets delegate history. The delegation evidences are used to record number of routing tasks assigned from upstream nodes. Trustor node can use this report for misbehavior detection.

| #fromHost | toHost | SigHashFrom | SigHashTo |
|---|---|---|---|
| P2 | P1 | d0482d1ca8a4a41e34dba28d5462aa66 | d0482d1ca8a4a41e34dba28d5462aa66 |
| P1 | P3 | 2638ecdc0a69dd73490af298e9943cfc | 2638ecdc0a69dd73490af298e9943cfc |
| P1 | P0 | 57837a019703410b1d178dd1dd22ad62 | 57837a019703410b1d178dd1dd22ad62 |
| P2 | P3 | b93f5876f41dfee41da44b6fc255e18 | b93f5876f41dfee41da44b6fc255e18 |
| P2 | P0 | e6e760c89c183dd67f6ed0e62b73d74d | e6e760c89c183dd67f6ed0e62b73d74d |
| P3 | P1 | a859441b04ab470d912a9068f6ff629b | a859441b04ab470d912a9068f6ff629b |

Fig.4 Delegation History

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

- **Forward History:** The time when one node forwards the message to next node forward history is created. As shown in Fig.5, node P2 forwards the packet to node P1, at that time the signature is generated. This report can be used by trustor at the time of misbehavior detection.

| MSG_ID | fromHost | toHost | Sig |
|---|---|---|---|
| M1 | P2 | P1 | d0482d1ca8a4a41e34dba28d5462aa66 |
| M2 | P1 | P3 | 2638ecdc0a69dd73490af298e9943cfc |
| M3 | P1 | P0 | 57837a019703410b1d178dd1dd22ad62 |
| M4 | P2 | P3 | b93f5876f41dfee41da44b6fc255e18 |

**Fig.5** Forward History

## VI. CONCLUSION AND FUTURE WORK

In this paper various trends of security in opportunistic networks are studied. Due to misbehaviour of node the performance of network affects and gives poor results. Designing a protocol for secure and trustworthy routing in an opportunistic network is one of the most interesting challenge. The secure routing in opportunistic networks can be achieved by the use of efficient routing protocol i.e. which has high delivery ratio and low content delay. We studied the mechanisms and explored techniques from some of the existing protocols in opportunistic networks that can efficient to for node misbehaviour detection with low transmission and signature verification cost using the probabilistic misbehaviour detection scheme.

## REFERENCES

1. Ing-Ray Chen, Fenye Bao, MoonJeong Chang, and Jin-Hee Cho, ”Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing”.IEEE Trans. Parallel and Distributed Systems, vol. 25,no. 5, May. 2014.
2. E. Ayday, H. Lee, and F. Fekri,”An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks”, IEEE Trans. Mobile Computing, vol. 11, no. 9, pp. 1514-1531, Sept. 2012.
3. M.K. Denko, T. Sun, and I. Woungang,”Trust Management in Ubiquitous Computing: A Bayesian Approach,” Computer Comm., vol. 34, no. 3, pp. 398-406, 2011.
4. E. Ayday, H. Lee, and F. Fekri,”Trust Management and Adversary Detection for Delay Tolerant Networks,” Proc. Military Comm. Conf., pp. 1788-1793, 2010.
5. S. Kosta, A. Mei, and J. Stefa,”Small World in Motion (SWIM): Modeling Communities in Ad-Hoc Mobile Networking,” Proc. Seventh IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks, June 2010.
6. N. Li and S.K. Das,”RADON: Reputation-Assisted Data Forwarding in Opportunistic Networks,” Proc. Second ACM Intl Workshop Mobile Opportunistic Networking, pp. 8-14, Nov. 2010.
7. A. Mei and J. Stefa, ”Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals,” Proc. IEEE Intl Conf. Distributed Computing Systems, pp. 488-297, June 2010.
8. Q. Li, S. Zhu, and G. Cao,”Routing in Socially Selfish Delay Tolerant Networks,” Proc. IEEE INFOCOM, pp. 1-9, Mar. 2010[8].
9. S.Trifunovic, F.Legendre, and C. Anastasiades,”Social Trust in Opportunistic Networks,” Proc. IEEE INFOCOM, pp. 1-6, Mar.2010.
10. A. Lindgren, A. Doria, and O. Schelen, ”Probabilistic Routing in Intermittently Connected Networks,” ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 7, no. 3, pp. 19-20, 2003.
11. A. Vahdat and D. Becker, Epidemic Routing for Partially Connected Ad Hoc Networks, technical report, Duke Univ., 2000.
12. K.S.Trivedi,”Stochastic Petri Nets Package User’s Manual,” Dept. of Electrical and Computer Eng. Duke Univ., 1999.

## BIOGRAPHY

**Anant Ravasaheb Khot** is a Post Graduate student in the Department of Computer Engineering, R. M. D. Sinhgad School of Engineering, Warje, Pune-58, India.