ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

Trust Management in Opportunistic Networks

Anant R. Khot[1], Prof. Vishal Mogal[2], Prof. Jyoti Raghatwan[3]

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]

Assistant Professor, Dept. of Computer, RMD Sinhgad School of Engineering, Pune, India[3]

ABSTRACT: Malicious and selfish behaviors represent a serious threat against routing in Opportunistic Networks. Opportunistic networks becoming dynamic research area in wireless communication.These 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. Due to the unique network characteristics, designing a misbehavior detection scheme in opportunistic network is regarded as a great challenge. In this paper, we propose a trust based probabilistic misbehavior detection scheme, for secure and trustworthy routing toward efficient trust establishment. This trust based mechanism can be useful to judge the node's behavior by the collected routing evidences and probabilistically checking. Additionally, with use of appropriate 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, Trust management.

I. INTRODUCTION

The Opportunistic Network 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 experience from frequent discontinuations, irregular links and continuously changing 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.

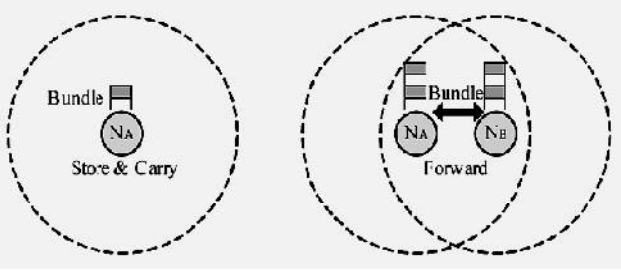

Fig1. Bundle store-carry- forward in DTN

II. RELATED WORK

Ing-Ray Chen et al have advised trust based routing protocol [1] by certifying direct trust and indirect trust among opportunistic nodes. This determination is done by evaluating the few trust properties (such as healthiness, unselfishness, connectivity and energy) of every meeting node.Healthiness, unselfishness and energy are considered to get maximum message delivery ratio, and connectivity to minimize message delay. In this scheme the level of trust of every node is assumed in [0, 1], where 0 indicates complete distrust and 1 represent complete trust. This way trust

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

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 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 maintaining 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 user's 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

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

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 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 suggested a routing protocol for sporadically 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.

Proposed algorithm

The mobile users can create a social network for instantaneous communication in Opportunistic network. In such network any node can misbehave or act as a selfish node while contents transferring. In opportunistic networks nodes can act with different kinds of behaviors as described below,

- **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.

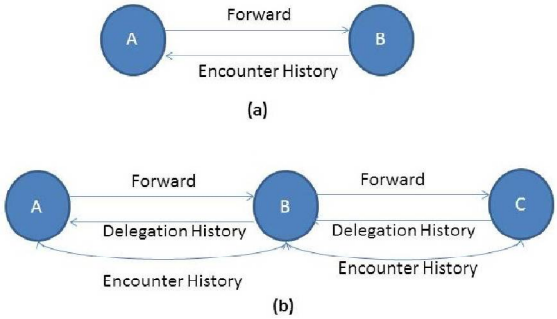

Fig2. System Design

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

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 history and delegation history and consequently A decide whether B is appropriate next node or not. In this case A act as Trustor and B as Trustee. In (b) A send contents 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 maintains and exchange crucial routing information such as Encounter history, delegation history and forward history. By using these kinds of information Trustor can assesses nodes behavior for selecting next hop to forward contents. We can get complete workflow of system design in Fig2. With the use of this trust based routing scheme Trustor can assess the trust with direct trust and indirect trust by using trust property X and routing history at time (t+dt) [1].

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.

Pseudo code: Basic Misbehavior Detection Algorithm
Here, j = node index.
stask = set of message forwarding requests.
sForward =set of message forwarded requests.
[t1,t2] = time period.
R = Set of contacted nodes.
D = Number of copies.
The algorithm used for the misbehavior detection is considered with the following Pseudo code:

```
procedure BASICDETECTION (( j, Stask, Sforward , [t1,t2],R,D))
for each m in Stask do
    if m not in Sforward and R!=0 then
        return 0
    else if m in Sforward and Nk (m) not in R then
        return 0
    else if m in Sforward and Nk (m) in R and ( Nk (m) ) less than D then
        return 0
    end if
    else
        return 1
```

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

end for
end procedure

III. EXPERIMENTAL RESULTS

We have used Eclipse as an implementation tool with Java as a programming language for designing opportunistic network environment and validating the trust based mechanism for misbehavior detection of node. Based on various movement models, the specific scenarios are created. We used the routing protocols available for opportunistic network such as Epidemic, PROPHET. The routing function is implemented by routing modules. The 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. Routing reports such as encounter history, Delegation history and forward history are generated through report generator. Each node has interface, persistent storage, movement, energy consumption and message routing. The nodes move according to movement models.

Opportunistic 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.

In trust assessment process, we defining important data forwarding reports that can be used to identify whether a node is a malicious one or not:

- **Encounter History:** It holds the information of nodes encounter each other, their generated signature. The MD5 algorithm used for generating signature. As shown in Fig.4, when the nodes c6 and d3 meet each other; to show the evidence of their meeting the signature is generated. In this way the encounter history is produced for all encountered nodes. This encounter history can be used by trustor node that holds trust authority at the time of misbehaviour detection.

EncounteredNodes		Signature
c6	d3	9e2d9c77ccf0a0b0e81fcf9d0a670793
c6	d5	2043e41a4b3d3b2ff68799947854a6f9
c6	p1	a000325ea65f39aad6d0d5a82480fa6b
p1	d4	de263d1718e054aaca472fb2b8e8d25
p0	d4	16460cf40deac8409143c1e02f6789a8
d4	p2	a072d887d2ad2fbaa0dc350c9289e27
d5	d3	4f617a882ebcc26fd3c0d6baa769bad1
d4	p2	1164b9239d0575ba170cb71a5e8ce618

Fig.4. **Encounter History**

- **Delegation History:**Delegation history holds information of nodes, their associated signature and tasks. When one node forwards the contents to next node then the next node gives the history back to its source node. As

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

shown in Fig.5, when the node p0 forwards the packet to d4 then node d4 gets delegate history. The delegation reportis used to record number of routing tasks assigned from upstream nodes. Trustor node can use this report for misbehaviour detection.

fromHost	toHost	SigHashFrom	SigHashTo
p0	d4	bf155c84c40330410b0b23a2e2e24aec	bf155c84c40330410b0b23a2e2e24aec
c6	p0	2806627a06ed5012b702aa248fe4798c	2806627a06ed5012b702aa248fe4798c
p2	p0	ea8daf1e8ddc986f22d3fbd6b701c74a	ea8daf1e8ddc986f22d3fbd6b701c74a
p1	d4	fda400af3fe8c52b56486de4a9ea2077	fda400af3fe8c52b56486de4a9ea2077
d4	d3	13cd4ae0067f2e6c6da7327800411fa2	13cd4ae0067f2e6c6da7327800411fa2
d3	p1	79e217b01648277d0fa85a7d1dab2e75	79e217b01648277d0fa85a7d1dab2e75
p2	d5	14d023100b4183bd7548a81dbe8cf144	14d023100b4183bd7548a81dbe8cf144
c6	d3	9b31536df5a606feb1ec051e5a73e05b	9b31536df5a606feb1ec051e5a73e05b

Fig.5. **Delegation History**

- **Forward History:**Forward history contains information of nodes, signature and contents forwarded. When one node forwards the message to next node forward history is created. As shown in Fig.6, 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 misbehaviour detection.

Message_ID	fromHost	toHost	Sig
M1	p0	d4	bf155c84c40330410b0b23a2e2e24aec
M2	c6	p0	2806627a06ed5012b702aa248fe4798c
M3	p2	p0	ea8daf1e8ddc986f22d3fbd6b701c74a
M4	p1	d4	fda400af3fe8c52b56486de4a9ea2077
M5	d4	d3	13cd4ae0067f2e6c6da7327800411fa2
M6	d3	p1	79e217b01648277d0fa85a7d1dab2e75
M7	p2	d5	14d023100b4183bd7548a81dbe8cf144

Fig.6.**Forward History**

- **Nodes Assessment:**Behaviour of nodes (such as Honest, Misbehaved) identified with the use ofprobabilistic misbehaviour detection mechanism by evaluating trust value as shown in Fig.7.

Node_Description	Nodes
Honest Node	p0
Honest Node	p1
Misbehaved Node	p2
Honest Node	d3
Honest Node	d4
Honest Node	d5
Honest Node	c6
Misbehaved Node	c7

Fig.7.**Nodes Assessment**

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 7, July 2017

IV. CONCLUSION

In this paper severalinclinations of security in opportunistic networks are studied. Network performance can affects due to the misbehaviour of node that may leverages to pooroutcomes. There is no any specific trustworthy routing protocol in opportunistic network so implementation of such secure and trustworthy routinga protocol in an opportunistic network is one of the most interesting task. We studied the mechanisms and appended techniques from some of the existing mechanisms in opportunistic networks.This trust based probabilistic misbehaviour detection mechanismcan be efficient for secure routing in opportunistic networksi.e. which can support high delivery ratio and low content delayand it can beeffectively used for node misbehaviour detection with short transmission and signature verification cost.

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.