International Journal of Advanced Information Science and Technology (IJAIST) *ISSN: 2319:268*
Vol.2, No.4, April 2013 *DOI:10.15693/ijaist/2013.v2i4.132-138*

Reputation Based Security Scheme In Dtn

Dr.A.Rajaram
Associate Professor/Department of ECE
Karpagam University, Coimbatore, India

Anooja.B
P.G. Scholar,Wireless Communication
Karpagam University, Coimbatore

***Abstract*— Disruption Tolerant Networks (DTN) differ from traditional network paradigms because of their inconsistent connectivity between nodes. Mobile nodes are often affected by malicious node during transmission. Detection of malicious node among the normal nodes is important in networks. The main objective of this work is to detect the misbehaving nodes using reputation based security scheme. The node calculates its packet dropping rate and if it is above the threshold level it is not chosen as a valid intermediate node. Once the presence has been identified, it will be isolated automatically by means of misbehaviour detection list table. Opportunistic data forwarding can be abused by an adversary by injecting spurious packets in order to waste the resources of the network. To guard against such attacks, it is important to authenticate packets at intermediate nodes. Packet authentication in itself comes with overheads such as computation cost and energy consumption which can be exploited by an attacker to mount a denial of service attack. RBSS acts as a vital security service for such malicious exploitation. It also implements an energy model through which node with lower consumption of energy is chosen for forwarding packets. Through simulations it shows that the proposed mechanisms can improve network performance and save considerable amount of power even in the presence of attackers. Simulation results in NS-2 shows that this security based system provides better detection efficiency, low energy consumption and low end-to end delay.**

Index terms -DTNs, Malicious, Mobility, RBSS, End-to end delay.

I. INTRODUCTION

A. Disruption Tolerant Networks (DTNs)

Disruption Tolerant Networking is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications.DTN routing usually follows "store-carry-forward;" i.e., when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards the packet.

In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks.

Routing misbehavior will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets.

B. Characteristics of DTN

The main nature of a DTN is shown below in Fig. 1

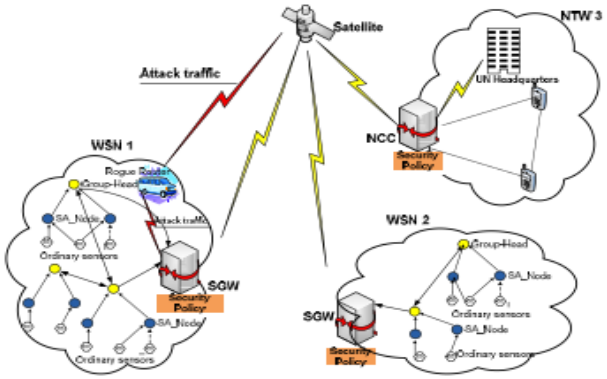

Fig.1.1 Disruption Tolerant Network:Heterogenous Network

Contact: A contact is an opportunity to send data over an edge. More precisely, it is a specific edge and a corresponding time interval during which the edge capacity is strictly positive. Messages Communication demands are represented by messages. A message is a tuple (u, v, t, m), where u is the source of the message, v is the destination, t is the time at which the message is injected into the system and m is its size (messages can be of arbitrary size). The set of all messages is called the traffic demand.

Storage : The nodes in a DTN have finite long-term storage (buffers) used for holding in-transit data or data waiting to be consumed by the application at a destination node. .

Routing: Routing occurs in a store and forward fashion. The routing algorithm is responsible for determining the next edge(s) that a message should be forwarded along. Messages not immediately forwarded wait until they are assigned to contacts by the routing algorithm.

II. RELATED WORK

In mobile ad hoc networks, much work has been done to detect packet dropping and mitigate routing misbehavior. To detect packet dropping, Marti *et al.* [16] proposed watchdog-based solutions in which the sending node operates in promiscuous mode and overhears the medium to check if the packet is really sent out by its neighbor. However, neighborhood monitoring relies on a connected link between the sender and its neighbor, which most likely will not exist in DTNs. In DTNs, a node may move away right after forwarding the packet to its neighbor, and thus cannot overhear

if the neighbor forwards the packet.

Another line of work uses the acknowledgement (ACK) packet [11] sent from the downstream node along the routing path to confirm if the packet has been forwarded by the next hop. Liu *et al.* [11] proposed a 2ACK scheme in which the sending node waits for an ACK from the next hop of its neighbor to confirm that the neighbor has forwarded the data packet. However, this technique is vulnerable to collusions, i.e., the neighbor can forward the packet to a colluder which drops the packet.

To mitigate routing misbehavior, existing works [16], in mobile ad hoc networks reduce the traffic flowing to the misbehaving nodes by avoiding them in path selection. However, they cannot be directly applied to DTNs due to the lack of persistent path.

In DTNs, one serious routing misbehavior is the black hole attack, in which a black hole node advertises itself as a perfect relay for all destinations, but drops the packets received from others. Li *et al.* [8] proposed an approach that prevents the forgery of routing metrics. However, if the black hole node in- deed has a good routing metric for many destinations, their ap- proach will not work, but our approach still works by limiting the number of packets forwarded to the black hole node.

Our solution has some similarity with previous work [3]. It doesn't provide any data authentication and confidentiality. Quinghua Li [1] proposed a mitigating routing misbehaviour scheme earlier which provides better routing performance in an efficient way. Our work is complementary since besides dealing with misbehaviour routing we also consider the data integrity and low energy consumption factors

III. EXISTING SCHEME

A. OVERVIEW OF THE PDSS SCHEME

In Packet delivery security scheme(PDSS), a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their contact records to avoid being detected, a small part of each contact record is disseminated to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes. This misreporting is referred to as replay-record.

This misreporting violates the consistency rules which are obeyed by normal nodes.

- Rule 1: use a unique sequence number in each contact
- Rule 2: For two records signed by the same node, the record with a smaller contact time also has a smaller sequence number.

After detection, the witness node floods an alarm via Epidemic routing to all other nodes. The alarm includes the two inconsistent summaries. When a node receives this alarm, it verifies the inconsistency between the included summaries and the signature of the summaries. If the verification succeeds, this node adds the appropriate misreporting node into a blacklist and will not send any packets to it. If the verification fails, the alarm is discarded and will not be further propagated. A misreporting node will be kept in the blacklist for a certain time before being deleted. Misbehavior routing can be mitigated by limiting the number of packets forwarded to the misbehaving nodes**.**

B. Disadvantages of the existing scheme

- Detection of misbehaving node is time consuming which decreases the efficiency of the scheme.
- Packet security is not provided and hence several attacks can be expected.
- Overhead & delay are high in this scheme.
- Energy consumption is more and hence reliability of the network is low.

IV. OVERVIEW OF THE PROPOSED WORK

A. Objectives

In this paper, we propose to design a secured and sheltered routing which can achieve the following objectives:

- Routing misbehaviour is mitigated by detecting the misbehaving nodes using reputation based system.
- Data intergity is maintained by a novel threshold cryptographic technique called Proactive secret sharing scheme.
- The overall reliability of the network is improved by choosing the minimun energy consumption nodes.

B. Overview of the proposed Mechanism

Here the packet dropping between the source and destination node is measured. Here the threshold value of node approval is set to find the packet dropping attacks. Generally effect of Denial of Service (DoS) attacks induces more packet dropping, misrouting the information and damage the whole network connectivity. In previous phase, the packet dropping in Disruption Tolerant Networks is proposed. Here, a new algorithm is proposed to find the DoS attacks.

The proposed scheme consists of the following modules

i. Detection of Packet Dropping Attacks
ii. Shared Secret Key Scheme
iii. Energy consumption model

C. *Packet dropping detection*

It is essential to detect the node which drops the packets .The procedure to find the misbehaving node is given below**.**

Step1:

Source node sends the data packet to the destination node via intermediate nodes.

Step 2:

Once the intermediate node receives the packet, first it will check the destination id, source id and sequence number. If the route id is not valid, then it will drop the packet.

Step 3:

Intermediate nodes also verify the packet dropping ratio which will be stored in the misbehavior list table.

The Packet Dropping Ratio is calculated by,

$$\frac{PacketsDropped}{TotalNo.ofPackets} x100 \quad (1)$$

Here, we have set the threshold dropping ratio t_{pdr}. If any packet dropping ratio is greater than the t_{pdr}, the whole route will be considered as invalid, otherwise valid.

Node approval is also used to identify the malicious behaviors. Evaluating the approvals is given by NR_R^P which is node P's evaluation to node P by collecting approvals,

$$NR_R^P = \frac{\sum_{f \in \psi} F|P \to Q| * F|R \to Q|}{F|P \to R|} \quad (2)$$

γ is a group of recommenders.

$F|P \to Q|$ is trust vector of node P to Q.

$F|R \to Q|$ is trust vector of node R to Q.

Invalid route ID, false node recommendation about neighborhood node and more packets dropping that indicates the presence of malicious node.

Once the presence has been identified, it will be isolated automatically by means of misbehavior detection list table. Thus the node is injected by means of DoS attack.

Step 4:

Once all the fields are verified, the intermediate node sends the Route Reply (RREP) packets to source, or any problem occurs, it will send the Route Error (RERR) packet.

Step 5:

Finally the destination node will check the no. of packets received. Thus the behavior of DoS attack can be successfully detected by means of proposed RBS scheme.

D. *Secret sharing scheme*

The concept of Proactive Secret Sharing (PSS) is used to provide data authenticity and confidentiality. In the PSS implementation, each share holder randomly generates own sub-shares (e.g., (s_{i1}, s_{i2}, . . . , s_{in}) on node i), and each sub-share is mutually exchanged to refresh own share. More precisely, the PSS procedure can be performed in the following steps:

1) Let (s_1, s_2, . . . , s_n) be an (n, t) sharing of the secret key S of the service, with node *l* having S_l.
2) Node *l* (i {1 . . . n}) randomly generates s_l's sub shares (s_{l1}, s_{l2}, . . . , s_{ln}) for an (n, t) sharing.
3) Every sub-share s_{lk} (k {1 . . . n}) is distributed to node k through secure link.
4) When node k gets the sub-shares (s_{1k}, s_{2k}, . . . , s_{nk}), it computes a new share from these sub-shares and its old share with an equation,

$$s'_k = s_k + \sum_{k=1}^{n} s_{lk} \quad (3)$$

After each PSS, all the shares will be changed, so that old shares become useless. In such case, since it is impossible to obtain new share from old share, a malicious node must collect at least t shares during the time between two executions of the PSS, which obviously makes it more difficult.

In the proposed scheme periodically PSS occur at start first any share holder node (master node) send pss_start flag to all other share holders (master nodes) and all that nodes now send pss_start_ack to the share holder that initiated the PSS procedure. After receiving pss_start_ack from all share holder nodes the initiating share holder node send refresh flag to all share holder nodes.

Now all nodes refresh its share and send the shares to other share holders using digital signature and encrypted with public key of destination node. After receiving share from all share holders the initiating share holder node now send pss_end flag to all other share holders and wait for ack.

After receiving pss_end_ack from all share holders the initiating node now send refresh end flag to all share holders. So now reach share holder can use these new shares for further communication of DTN.

E. *Energy consumption model*

Energy conservation is an inevitable factor in networks. To ensure a high performance network scenario, we need to consider the energy model of the network.
The energy model of proposed algorithm is given below. In this model energy consumption for transmitting M bit is equal to:

$$E_{tr}(M, d) = E_{elec} \times M + \delta_{amp} \times M \times d^2 - E_{wast}(P_{drop}) \quad (4)$$

M = bit contain some information like current energy level of the node, data label, node's location and hop count.
E_{elec} = Energy to be Transmitted and Received electronic device module (75 nJ/bit)
δ_{amp} = Transmitter Amplifier (150 pJ/bit/m^2)
d = distance between the two nodes.
$E_{wast}(P_{drop})$ = Energy wasted on packet dropping

And the energy for receiving K bit is equal to:

$$E_{rr} = E_{elec} \times M \quad (5)$$

In this energy consumption model, each node has its own energy status to verify the energy consumption of neighbor nodes and path energy.

If the node had minimum energy consumption of nodes and path that route is considered as efficient route and node. First the energy consumption of transmitting node is calculated. Energy wasted on packet dropping is estimated from the packet dropping ratio.

The proposed algorithm determines the energy conservation rate based on the above three factors and also the total number of bits transmitted per energy

$$E_{CR} = \sum (T_{mb}, T_{tv}, DS_{\min}) + \frac{\chi_{BR}}{\sum \delta_{es}(t)} \quad (6)$$

χ_{BR} - Number of bits transmitted (bits).

$\sum \delta_{es}(t)$ - Total energy consumed (Joules).

T_{mb} – Trust Mobility factor

T_{tv} – Trust threshold vector value

DS_{min} - Minimum value of Digital Signature

From the analysis of the proposed scheme, the energy efficiency of the node is well improved and the data integrity of the networks is getting more.

V. ADVANTAGES OF THE PROPOSED WORK

A. Packet Dropping and Misrouting the information:

In routing discovery phase, with the intention of dropping packets the malicious node announces that it has a valid route to the destination node, but this route is fabricated.

In packet transmitting phase, the source sends packet to destination node, the malicious sits among the nodes and misroutes the packets from source to destination node. With the RBSS we can know that detect a malicious node even before forwarding the packets to it because of its dropping rate RP value. This enhances the mitigation of routing misbehaviour.

B. Suppressing the communication between the nodes:

In data forwarding phase, the attacker absorbs the data packets which are supposed to be forwarding to next-hop node. Therefore, communications of nodes are totally suppressed. An even more subtle form of attacks is that attackers can selectively forward packets; thereby their malicious behaviors are not so easy to be detected. Using PSS security scheme, Packets are made secured increasing the overall performance of the network.

C. Energy conservation:

packet authentication itself comes with overheads such as computation cost and energy consumption which can be exploited by an attacker to mount a denial of service attack. Hence calculation of energy of nodes is an important factor and deactivating low energy nodes is being done. Hence the reliability of the network is ensured.

VI. PERFORMANCE EVALUATION

A. *Simulation Model and Parameters*

We use NS2 to simulate our proposed algorithm. In our simulation, 100 mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 100 meters. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1.

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	100m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	80
Mobility Model	Random Way Point

B. *Performance Metrics*

We evaluate mainly the performance according to the following metrics.

Average Packet Consumed Energy: It is the ratio of the total time taken for packets received successfully and the total number of packets transmitted.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

End-to-end-delay : The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Misbehaving detection ratio: The number of misbehaving nodes to that of total nodes gives the misbehaving detection ratio.

B. *Results*

The comparison graph of existing packed delivery secured scheme (PDSS) is compared with the proposed scheme RBSS ie Reputation Based Security Scheme.

No defense scheme and optimal scheme are also considered here. No-defense Scheme is the one that doesn't deal with routing misbehaviour. Optimal Scheme assumes that all misbehaving nodes are known and no packet is forwarded to them.

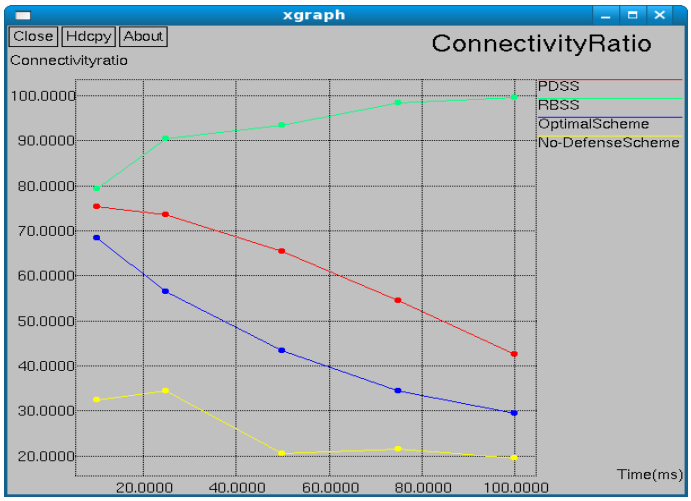

Fig. 2 Connectivity ratio vs time

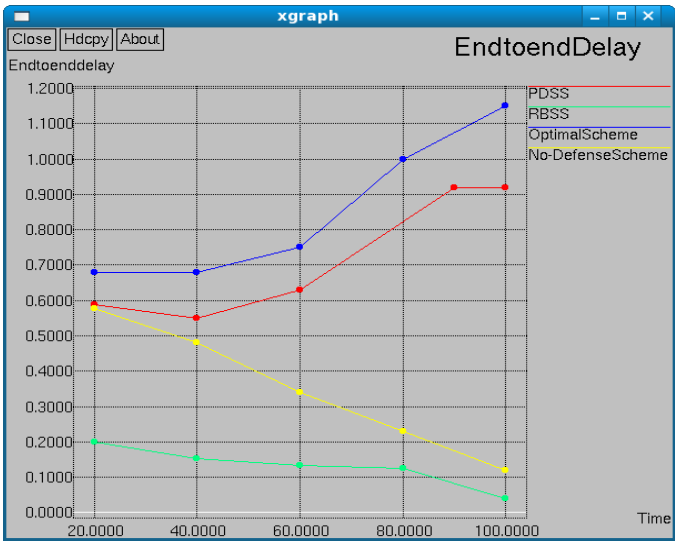

Fig. 5 End to End delay vs time (Sec)

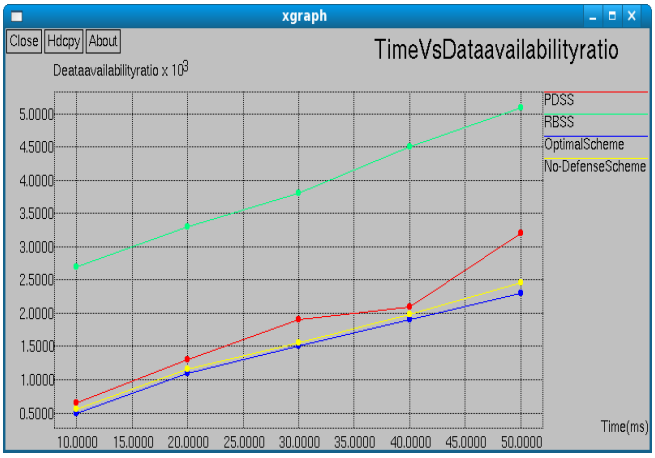

Fig.3 Data availability ratio vs time

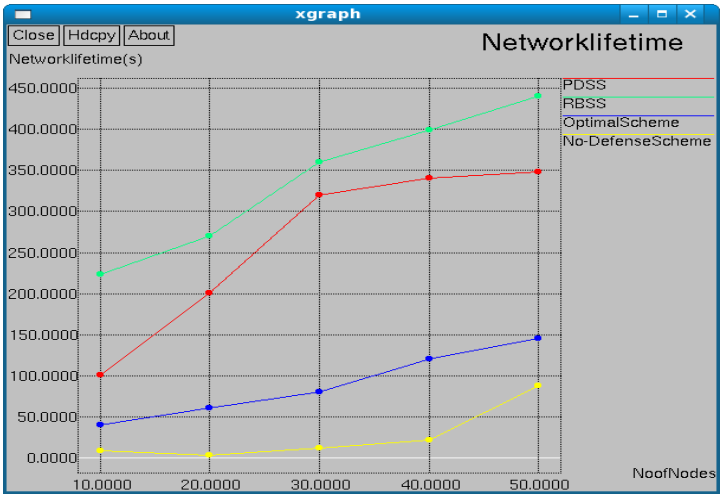

Fig.6 Network life time vs No: of nodes

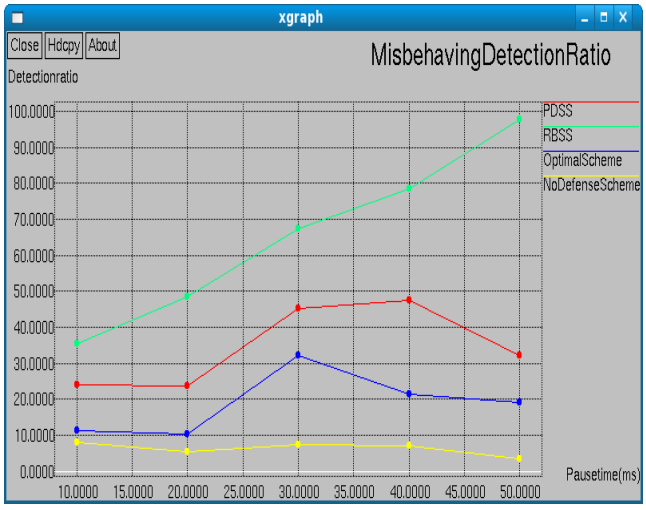

Fig. 4 Misbehaving detection ratio vs pausetime

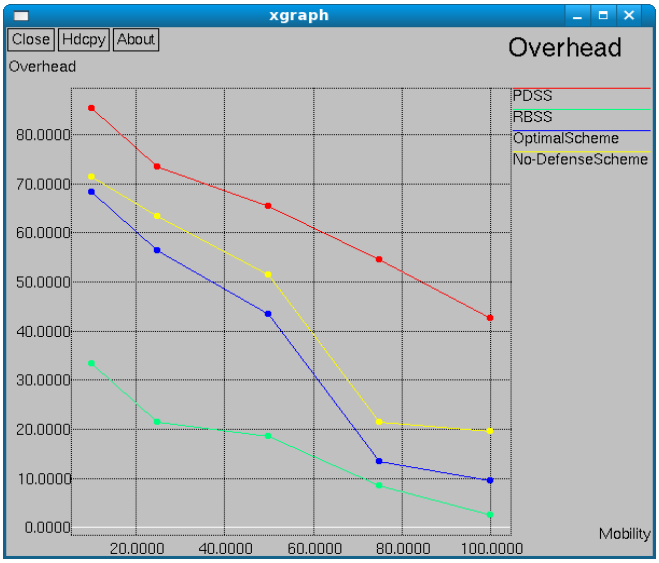

Fig. 7 Overhead of RBSS and PDSS

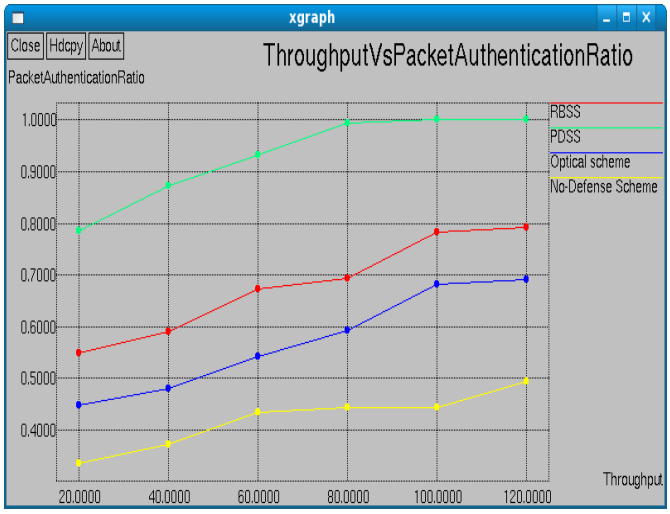

Fig. 8 Packet authentication ratio of PDSS Vs RBSS

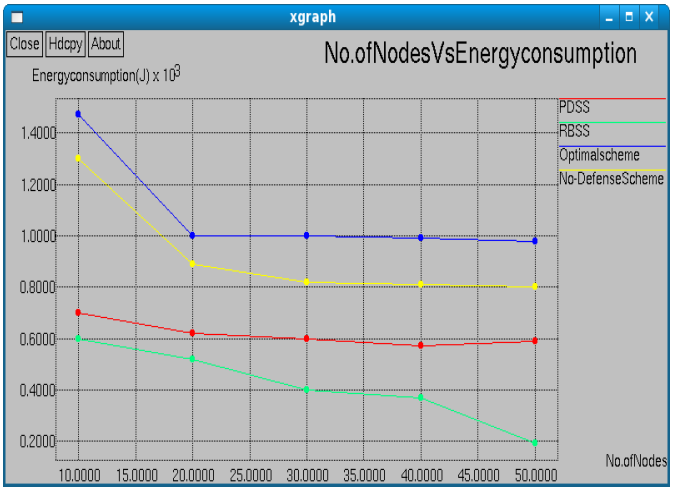

Fig.9 Energy consumption of nodes in RBSS Vs PDSS

It is clear from the above results that more number of nodes with packets of very low overhead and with very low energy consumption is available in the network increasing its lifetime and maintains a very low delay.

VII. Conclusion and Future Enhancement

The proposed scheme is very generic and it does not rely on any specific routing algorithm. This scheme is simple and efficient. It uses reputation system to detect the misbehaving nodes and enhances the reliability of the overall network by conserving the energy of the unavailable nodes by deactivating them. It also ensures a secured data forwarding with the Proactive Secret Sharing Scheme. This scheme makes balance between the energy consumption, misbehaviors and data integrity. In this scheme nodes use very low energy consumption for detecting misbehaving node. Trace-driven simulations show that this solution is efficient and can effectively mitigate routing misbehavior.

The further enhancement can be done by providing security to the contact node .This avoids the contact node being compromised by malicious node to avoid being detected. Mitigating routing misbehaviour and enhancing packet delivery ratio can be done through various other trust based mechanisms. Better security schemes and energy models can be implemented to improve the trace driven simulation results of the reputation based security scheme.

References

1. Qinghua Li,Guohong Cao, “Mitigating routing misbehaviour in disruption tolerant networks”,in IEEE transactions on Information forensics and security,Vol.7,No.2,April 2012 .
2. Qinghua Li,Wei Gao, Sencun Zhu, Guohong Cao , “Routing in socially selfish delay tolerant network”, in Elsevier,Sciverse Science Direct,2012,pg. 1619-1632.
3. Gianluca Dini, Angelica Lo Duca, “Towards a reputation based routing protocol to contrast blackholes in a delay tolerant network”, in Elsevier,Sciverse Science Direct,2012,article in press.
4. Chauhan Gargi K, “Proactive secret sharing scheme for mobile ad-hoc networks”, in Int.J.Comp.Tech.Appl,Vol 2(6),4003-4006,Nov-Dec 2011
5. Q. Li, W. Gao, S. Zhu, and G. Cao, “A routing protocol for socially selfish delay tolerant networks,” in Ad Hoc Networks, Aug. 2011, DOI:10.1016/j.adhoc.2011.07.007.
6. W. Gao and G. Cao, “User-centric data dissemination in disruption tolerant networks,” in Proc. IEEE INFOCOM, 2011, pp. 3119–3127.
7. G.Ansa,H.Cruickshank and Z.Sun, “An energy efficient technique to combat DOS attacks in delay tolerant networks”, in Elsevier,Sciverse Science Direct,2010,pg. 1619-1632.
8. F. Li, A. Srinivasan, and J. Wu, “Thwarting blackhole attacks in dis-truption-tolerant networks using encounter tickets,” in Proc. IEEE IN-FOCOM, 2009, pp. 2428–2436.
9. V. Erramilli, A. Chaintreau, M. Crovella, and C. Diot, “Delegation forwarding,” in Proc. ACM MobiHoc, 2008, pp. 251–260.
10. J. Burgess, G. D. Bissias, M. Corner, and B. N. Levine, “Surviving attacks on disruption-tolerant networks without authentication,” in Proc. ACM MobiHoc, 2007, pp. 61–70.
11. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no.5, pp. 536–550, May 2007. A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, “Lowcost communication for rural internet kiosks using mechanical backhaul,” in ACM Proc. Mobicom, 2006, pp. 334–345
12. N. Eagle and A. Pentland, “Reality mining: Sensing complex social systems,” Pers. Ubiquitous Comput., vol. 10, no. 4, pp. 255–268, 2006.

13. J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in Proc. IEEE INFOCOM, 2006, pp. 1–11.
14. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in IEEE Symp. Security and Privacy, 2005, pp. 49–63.
15. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000, pp. 255–265.
16. A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks Duke University", Tech. Rep. CS-200006, 2000

Authors Profile

Dr.A.Rajaram received the **B.E.** degree in electronics and communication engineering from the Govt. College of Engineering, Salem, Anna University, Chennai, India, in 2007.Currently doing **M.E.** in electronics and communication engineering (Communication Systems) in Anna University of technology, Coimbatore, India. His research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks ,Neural Networks and fuzzy logic, Communication networks

Anooja.B received the **B.E.** degree in electronics and communication engineering from VPMM Engineering college for women, Srivilliputtur, Anna University, Chennai, India, in 2008.Currently doing **M.E.** in electronics and communication engineering (wireless communication) in Karpagam University, Coimbatore, India. Her research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks and Communication networks