A SURVEY OF MISBEHAVIORS OF NODE AND ROUTING ATTACK IN DELAY TOLERANT NETWORK

Sarawagya Singh
Student,department of of information technology,veltech Dr.RR&Dr.SR Technical unviversity
sarawagya@gmail.com

Elayaraja.K
Student, department of information technology ,veltech Dr.RR&Dr.SR Technical unviversity
kelaya5@gmail.com

ABSTRACT: Delay tolerant network is the new types of network that suffer lacks of connectivity between source and destination.DTN is a network that constructed to maintain communication in the most uncertain and accent environment.. DTN is a new types of network and different from other kinds of networks. A misbehavior and attacks are threat to any kind of networks. A misbehavior can reduce the performance of any kind of networks. Misbehavior of node means that a node not performs its duties in a proper way. There are two types of misbehavior of node in DTN are selfish node and malicious node. Selfish node is try to maximize their own gain by relish service provided by DTN while decline to onward the bundle for other. Malicious node that drop packet or customize packet to launch attacks. In the network Attack is any try to damage, leak, change, harm or gain unauthorized access. Attack can damage the network and launch the several types of attacks are black hole attack, Gray attack, wormhole attack. In this paper mainly focus on misbehavior of node and attacks in DTN. This paper help to know about the DTN network and information about misbehaviors and attack in DTN network.

Keywords: DTN, selfish node, malicious node, attack, misbehavior

1 INTRODUCTION

In delay tolerant network Communication is possible even if end-to-end connectivity is never achievable. DTN Exploiting node's mobility and using store-carry-forward fashion. this is a new types of network are different from other kinds of networks. Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack of continuous network connectivity. Disruption may exist because of the limits of wireless radio range, lack of mobile nodes, energy sources, attack, and noise. Delay tolerant network are those operating in mobile or extreme terrestrial domains, or planned networks in space. Delay tolerant network providing a convenient mode of communication for civilian and business purposes, DTNs networks are highly desirable for use in battle zones, relief efforts in remote area, and difficulty situations in disaster areas. In such cases, where no network infrastructures exist, DTNs network can provide a crucial mode of communication. Delay and disruption-tolerant networks (DTNs) are characterized by their lack of connectivity, resulting in a insufficiency of spontaneous end-to-end paths. A network of local networks supporting interoperability among them. An overlay on top of regional networks including the Internet accommodate long delays between and within regional networks and translate between regional network communication characteristics. The problems of DTNs can be affected by store-and-forward massage switching DTN routers need persistent storage for their queues because a communication link may not be available for a long time One node may send or receive data much faster or more reliably than the other node A message once transmitted may need to be retransmitted for some reasons. Assume communicating devices (nodes) in motion and or operation with limited power. When nodes must conserve power or preserve secrecy links are shut down -> intermittent connectivity network partition. On the Internet infrequent connectivity causes loss of data while DTNs disconnect delay with a store-and-forward approach. Network nodes may need to broadcast or connect during opportunistic contacts in which a sender and receiver make contact at an unscheduled time. The bundle layer a new protocol layer overlaid on top of heterogeneous region-specific lower layers with which application programs can communicate across multiple regions. Mainly nodes in DTNs are of two types which are more different from other networks.

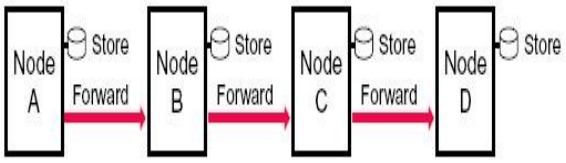

Fig: 1 a node store and forward in DTNs

Selfish nodes minimize their contributions to the network community and maximize their own gains by placing conniving nodes into the network community (to grab information). Malicious nodes attack proper network operations and do not consider their own gains. DTNs security protocols have to be more invulnerable and powerful to

ISSN: 2278 – 7798

handle these types of nodes. Also the characteristics of DTNs and characteristics of mobile ad-hoc networks are distant which makes these security protocols ineligible for DTNs. DTN-specific security solutions are required. Therefore, traditionally security system is not suitable. Messages in DTNs are called as bundles. They traverse through Delay Tolerant Network bundle agents who partake in bundle communications to form the DTN store-and-forward overlay network. Misbehave mean that to behave badly or improperly. In the adhoc network that totally depend upon the each other node for exchange of information. Misbehave in network that node not perform its task in a proper way. In computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. in this paper mainly focus on gray hole attack,blackhole attack and wormhole attack .these attack are harmful attack against the DTN network.. Gray hole is a node that can transformation from behaving correctly to behaving like a black hole and it is literally an attacker and it will act as a normal node. black holes is an attack in the network where incoming or outgoing traffic is silently discarded (or "dropped") without informing the source that the data did not reach its intended recipient. worm hole attack are a network that mine information to another network, that is it get the data from one network replicate it into another network through tunnel . DTNs network are suffer from lack of contemporaneous, end-to-end path High variation in network conditions, Difficulty to predict mobility, patterns Long feedback delay.

2 DTN ROUTING MISBEHAVIOUR:

Misbehavior in network mean a node not performs its duties in a proper and behaves badly that effect on network performance. Dropping packets intentionally and significantly reduce the packet delivery rate, serious threat against network performance of DTN. a node could misbehave by dropping packet willfully even when it has potential to forward the data. They have plentiful buffer and meeting opportunities. Present misbehavior detection schemes for DTNs is Based on forwarding history verification.

2.1 Selfish misbehavior:

Intention is to save capacity, memory and CPU cycle.

2.2 Selfish misbehavior can be of two types:

2.2.1 Self-exclusion:

a selfish node does not perform when route discovery protocol is done to save its own power. self-exclusion mean that node is not perform at the route discovery protocol and not carry any packet during this time period.

2.2.2 Non-forwarding:

a selfish node aid in the route discovery process but drops data packets in the routing phase. Given a packet at a node, finding which output port it needs to go to is called “forwarding” – it is a per-node behavior, whereas routing may encircle several nodes. The forwarding function is performed by every node in the network including moderator, repeaters, bridges and routers.

2.3 selfish nodes:

In the real world most people are selfish and selfish user usually willing to help other with whom he has social ties. Because he has got help from them in the past or will probably get help from them in future. A social tie means an interpersonal tie that is fall into strong or weak category. Social ties, a selfish user may give difference prefernce.he is willing to provide better service to those with strong ties than those with weaker ties. Social selfish will effect on node behavior. Selfish node do not forward other packets, thus enlarge their gain at the overhead of all other. They are assumed to always behave rationally, so they cheat only if it gives them on advantage.

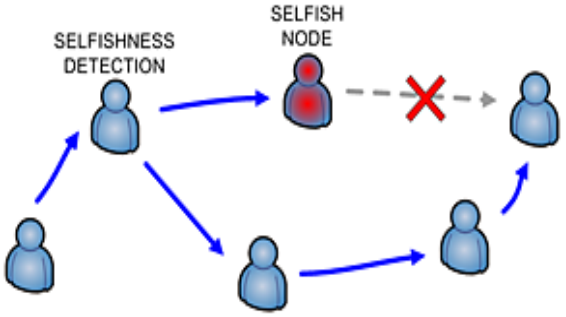

Fig2:selfish node

In ad hoc network it does not rely on a pre existing infrastructure,such as routers in wired networks or access points in managed wireless networks.ad hoc network is a peer to peer network of wireless nodes where nodes are needed to execute routing activity to provide end to end related among nodes. As mobile nodes are strained by battery power and bandwidth, some nodes may behave selfishly and refuse forwarding packets for other nodes,even though they await other nodes to forward packets to keep network connected. Selfish nodes do not ahead data or control packets for other nodes and the second, selfish nodes put off their network combine card when they have nothing to broadcast.An ad-hoc network is a local area network that is built spontaneously as devices connect.Instead of relying on a base station to equalize the flow of messages to each node in the network,the specific network nodes forward packets to and from each other.

2.4 Malicious node:

malicious nodes are present in a delay tolerant network,they may attack to diminish network connectivity by pretending to be coordinated but in effect dropping any data they are meant to allow. These actions may result in defragmented networks, detached nodes, and drastically reduced network completion.We aim to evaluate the added effect of the presence of malicious nodes on DTN network performance. packet delivery cannot be assure even when malicious nodes are not present, and resending data packets does not provide a good solution.

ISSN: 2278 – 7798

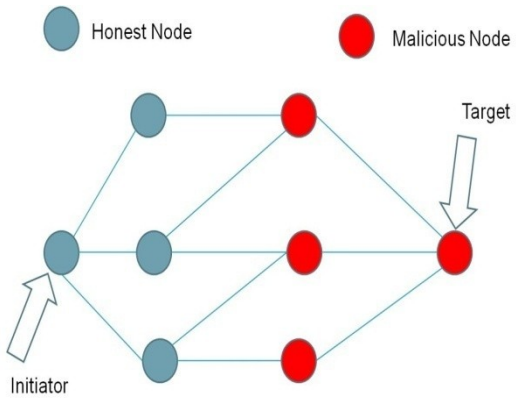

Fig3: malicious n

The simulation experiments examined various network conditions, including node density, movability speed, transportation power, and geographical circulation of devices. The simulation results determine that the existence of only one malicious node in a MANET can cause an added packet loss of more than 25%. With multiple rogue droppers, nearly 60% of data packets could be vanished. In such cases, the existence of malicious nodes have serious security indication.

2.5 Malicious behavior:

the main intention of Malicious behavior is to attack and damage the network.misbehavior is a major problem for any kinds of wireless networks. All the network suffer from this problem, because misbehavior a badly effect on the network performance and its efficiency.

2.5.Malicious misbehavior can be of two types:

2.5.1 Forwarding misbehavior:

packet lost, alteration,forgery,timing intrusion, silent route change etc.

2.5.2 Routing misbehavior :

route salvaging,lost of error messages forgery of error messages,strangely frequent route updates, sleep deprivation,blackhole,grayhole,wormhole attacks etc.

2.6 Routing misbehavior

2.6.1 Timing misbehaviour attack :

malicious node delays packet forwarding to secure that time-to-live (TTL) of the packets are expired so that the packets do not reach the destination. the malicious node mainly hold the packet until the it expire it TTL time period before reachnig the destination.

2.6.2 silent route change attack:

a malicious node promotes a packet through a various routes than it was intended to go through. in this silent route change malicious node promote packet to various routes and after that malicous node move through it.

2.6.3 route salvaging attack:

a malicious node re-routes packets to avoid a broken link, although no error actually has taken place. Route salvaging attacks are launched by the greedy internal nodes in the networks. Generally in mobile ad hoc network, there is no proper assurance that each transmitted packet will effectively reach the preferred destination node. As the adversaries make attack in the network and possible network failures can cause the packet to be damaged. salvage the packets from such loss, misbehaving internal nodes might duplicate and retransmit their packets even though no-sending-error messages are received. If many selfish nodes exist in the network, those nodes will make severe route salvaging attacks.

2.6.4sleep deprivation attack :

a malicious node sends enormous number of packets to another node so as to consume computation and memory resources of the latter. The attacker node makes the path node busy by sending the unnecessary packets to it. Hence the battery power of path node is drained off unnecessarily. With the aid of unnecessary routing packets flooding, the targeted node launches the sleep deprivation attacks in the network

3. TYPPES OF ATTACK IN DELAY TOLERANT NETWORK:

While a wireless network is more versatile than a wired one, it is also more accessible to attacks. This is due to the very nature of radio communications, which are made on the air. We now focus on attacks against the routing protocol in ad hoc networks. These attacks may have the aim of customize the routing protocol so that traffic flows through a particular node controlled by the attacker. An attack may also aim at gathering the formation of the network, making normal nodes store incorrect routes, and more generally at unsettling the network topology, an attack can be threat for any network especially for those who are without Infrastructure .DTN network have also no Infrastructure and provide information one location to another location. there are several types of attack in DTN network. We are mainly focus on main attack are black hole attack, ray hole attack, wormhole attack.

3.1 Blackhole attack:

The blackhole attack is one of the well-known security threats in wireless mobile ad hoc networks .In the DTNs network where coming or outgoing traffic is silently discarded ("or dropped"),without informing the source that the data did not reach its intended recipient.When checking the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic. The destruction is directly related to the likelihood of an adversary being selected as part of the route and attacker selectively drops only data packets, but still aid in the routing protocol

ISSN: 2278 – 7798

correctly. a black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead removes them. This normally occurs from a router becoming compromised from a number of different causes.

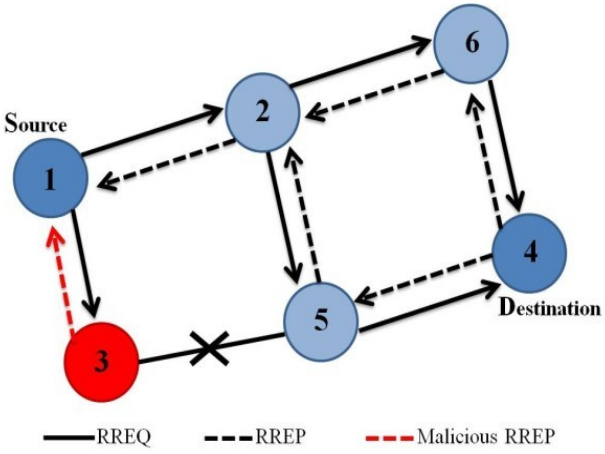

Fig: 4 black hole attack

One matter mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely lost from a damage network, the packet drop attack is very hard to recognize and avoid. The packet drop attack can be frequently deployed to attack in wireless ad hoc networks. as wireless networks have a much distant architecture than that of a typical wired network, a host can advertisement that it has the shortest path towards a destination. A kind of DOS where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to disturbance.This unfriendly node advertises its availability of fresh routes irrespective of checking its routing table.In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it .In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node,hence a malicious and spurious route is created. When this route is authorize, now it's up to the node whether to drop all the packets or forward it to the unknown address**.** a malicious node allegations to have the shortest path, but when asked to forward the packets, it drops them**.**

3.1 .1 LOCAL MONITORING IN BLACKHOLE ATTACK CAN DETECT:

Packet fake: An outgoing packet that has no corresponding incoming packet**.**

Packet alteration: Difference between the incoming and outgoing packet fields**.**

wilful packet delay: A packet was forwarded after a threshold time instead of immediately.

Packet lost: Packets were not forwarded within a maximum acceptable timeout threshold.

3.1.2 Two types of black hole attack

3.1.2 Internal attack:

This type of black hole attack has an internal malicious node which fits in between the directions of given source and destination. As soon as it gets the incidental this malicious node make itself an active data direction element. At this stage it is now able of operating attack with the start of data communication. This is an inner attack because node itself belongs to the data route. Internal attack is more accessible to secure against because of difficulty in detecting the internal misbehaving node. An internal attack occurs when an individual or a group within an organization seeks to disturb operations or exploit organizational all in all. In many cases, the attacker handles a refined amount of resources, mechanism and intelligence to launch a refined computer attack and potentially remove any evidence of that attack as well. One of the best ways to protect against internal attacks is to implement an intrusion detection system and to configure it to scan for both external and internal attacks. All design of attacks should be admit, and the logs should be analysed frequently. In internal attack, the attacker needs to gain the access to participate in the network activeness. Here the attacker comes with some malicious impersonation to get access from network as a new node.

3.1.3 External attack:

External attacks substantially halt outside of the network and deny access to network traffic or creating congestion in network or by disrupting the full network. External attack can become a kinds of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attacks can be summarized in following points**.** the attacker intents to cause traffic jam in the network which can be done by propagating fake routing information or to disturb the nodes from providing services .The attacker always disrupts the nodes to avail the services.

1. Malicious node discloses the alive route and notes the end address.

2. Malicious node sends a direction reply packet (RREP) including the destination address.

ISSN: 2278 – 7798

field spoofed to an unnamed destination address. Hop count value is set to lowest

values and the arrangement number is set to the highest value.

3. Malicious node send RREP to the nearby accessible node which belongs to the alive

route. This can also be send precisely to the data source node if route is available.

4. The RREP received by the nearby accessible node to the malicious node will relayed

via the fixed inverse direction to the data of source node.

5. The new info received in the route reply will allow the source node to amend

its routing table.

6. New direction selected by source node for selecting data.

7. The malicious node will vanish now all the data to which it exist in the route.

3.2 Gray hole attack:

In this kind of attack the attacker misleads the network by agreeing to forward the packets in the network. As soon as it gain the packets from the neighboring node, the attacker lost the packets. This is a type of alive attack. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it earn the packets it starts dropping the packets and launch Denial of Service attack. The malicious action of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it is very difficult for the network to figure out such kind of attack.Gray hole attack is also described as node misbehaving attack.

A relevance of black hole attack is the gray hole attack, in which the nodes will missed the packets choosy. Selective forward attack is of two types they are

1.Dropping all UDP packets while forwarding TCP packets.

2.Dropping 50% of the packets or dropping them with a probabilistic delivery. These are the attacks that seek to disturb the network without being disclosed by the security measures.

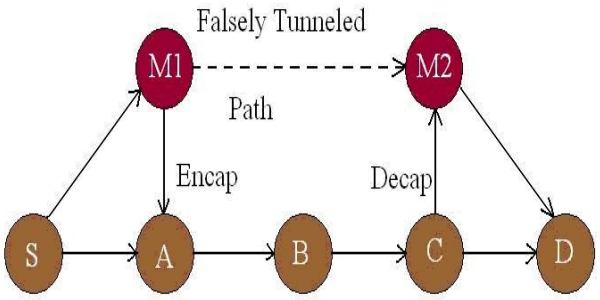

Fig:5 gray hole attack

Gray hole is a node that can alterations from behaving correctly to behaving like a black hole that is it is absolutely an attacker and it will act as a normal node. we cannot classify easily the attacker since it behaves as a routine node. Every node mange a routing table that stores the next hop node information which is a route packet to destination node. If a source node is in need to route a packet to the destination node it uses a exact route and it will be verified in the routing table whether it is available or not. the nodes has been dropped the interrupted packets with a certain probability and the detection of gray hole attack is a challenging process. commonly in the gray hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack. The other name for Gray hole attack is node misbehaving attack.

3.3 Wormhole attack:

a wormhole is an out-of-band communication, controlled by the adversary, between two physical locations in the network.In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another ends point in the network, and then response them into the network from that point. For tunneled areas longer than the normal wireless transmission range of a single hop, it is straightforward for the attacker to make the tunneled packet arrive with better metric than a normal multihop route. ad hoc networks that is particularly challenging to secure against. The wormhole attack is possible even if the attacker has not settled any hosts, and even if all connection provides authenticity and acquaintance. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and broadcasts them there into the network. The wormhole attack can form a sincere threat in wireless networks,notably against many ad hoc network routing protocols and location-based wireless security systems.

ISSN: 2278 – 7798

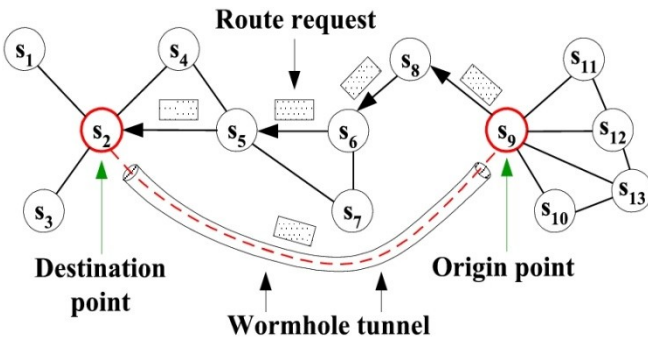

Fig: 6 worm hole attack

The adversary installs radio transceivers at both ends of the wormhole. It transfers packets (possibly selectively) received from the network at one end of the wormhole to the other end via the out-of-band contacts, and re-injects the packets there into the network. Adversary's transceivers are not regular nodes. Adversary doesn't need to understand what it tunnels (e.g., encrypted packets can also be tunneled through the wormhole). it is an easy to mount a wormhole and it may have devastating effects on routing. In Wormhole attack if more than one node is compromised, is reasonable to assume that these nodes interact in order to gain an additional advantage. This allows the adversary to perform a more effective attack. In Wormhole attack two adversaries collude by tunneling packets between each other in order to create a shortcut (or Wormhole) in the network. The attacker can send a route request and discover a direction across the ad hoc network, then tunnel packets through the non-adversarial nodes to execute the attack. Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on detecting the network, record the wireless data.

CONCLUSION

In this paper, we have described about misbehavior of node that is harmful for any kind of wireless network and also focus on the novel and powerful attack against the delay tolerant network. we mainly focus on the attack are black hole attack,gary hole attack and worm hole attack. This paper helps to know about the nature of the attack and help to prevent the attack in future.

REFERENCES

[1] " The Sybil Attack in Sensor Networks: Analysis & Defences": James Newsome, Elaine Shi, Dawn Song , Adrian Perrig 2009

[2] Routing in Socially Selfish Delay Tolerant Networks" Qinghua Li, Sencun Zhu, Guohong Cao .2010

[3] Pi: A Practical Incentive Protocol for Delay Tolerant Networks" Rongxing Lu, Xiaodong Lin, Haojin Zhu IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 9, NO. 4, APRIL 2010

[4] "Detection and Avoidance of Routing Attack in Mobile Ad-hoc Network using Intelligent Node"Abhiskek Ranjan, Venu Madhav Kuthadi, Rajalakshmi Selvaraj, and Tshilidzi Marwala,International Conference on Information Technology and Computer Systems Engineering (ITCSE'2013) Nov. 27-28, 2013 Johannesburg (South Africa)

[5] Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information,Ritesh Maheshwari, Jie Gao and Samir R Das Department of Computer Science, Stony Brook University Stony Brook, NY 11794-4400, USA

[6] A Study on Wormhole Attacks in MANET, Reshmi Maulik and Nabendu Chaki International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279

[7]A Survey on Gray Hole Attack in MANET V. SHANMUGANATHAN Mr.T.ANAND M.E.,IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012

[8] Analysis of Black Hole and Wormhole Attack using AODV Protocol, Shefi Mehta , Dr. Mukesh Sharma ,International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264) Vol. 1; No. 1, June 2013

[9] Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks" Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker

[10] A DTN Approach to Satellite Communications Carlo Caini, Member, IEEE, Piero Cornice, Rosario Firrincieli, and Daniele Lacamera, Student Member, IEEEIEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 26, NO. 5, JUNE 2008

[10] A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment
in Delay-Tolerant Networks Haojin Zhu, Member, IEEE, Suguo Du, Zhaoyu Gao, Student Member, IEEE, Mianxiong Dong, Member, IEEE, and Zhenfu Cao, Senior Member, IEEE, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 1, JANUARY 2014

ISSN: 2278 – 7798