An Augmented Approach for Secure and Reliable Routing in Mobile Ad hoc Network under Flooding Attack

Hardik Vyas, Ashish Revar
Department of Computer Science,
Marwadi University. Rajkot, Gujarat, India

***Abstract*— In this proposed approach, Denial of Service (DoS) attack is highly concentrated, which is caused by means of Flooding attack. This case is considered because all the other attacks can be easily identified and also be recovered, but this kind of Flooding cannot be easily traceable. So that in this system, a new routing protocol strategy is defined by means of Route Request and Route Response Strategies with the help of AdHoc Disjoint Vector (AODV). Source Node sends Route Request to the nearby node. The nearby node checks the request and sends the Route Response to Source Node back within a proper interval. The proper and relevant response from the neighbor node indicates it as a proper node as well as the neighbor node sequence Number will get incremented by 1. The node is proper then only the count will be incremented otherwise it consists attack content. This kind of nodes are properly blocked from the present scenario and the source checks for the alternate or other neighbor nodes to proceed for further communications. As per the regular network strategies the node selection or path selection process is purely based on Shortest Path Routing methodology. Apart from this scenario, a new scheme is introduced to recover the fault nodes by means of Fault Node Recovery Algorithm, which helps to recover the affected nodes by means of allocating the required bandwidth and energy to the affected nodes and make them as live for further communications.**

***Index Terms*—Wired, wireless, secure, attack, protocols, Mobile ad-hoc networks, Denial of service attack.**

I. INTRODUCTION

The main motto of this project is to find and resolve the vulnerable attacking called Flood, which are presented into the network region and try to affect data by DOS scheme while transmissions. Mobile Ad-Hoc Networks (MANET) a fast growing network scheme and it provides lots of features to communication strategies and routing protocols. Theses routing protocols are introduced to avoid the attacker nodes and provides the efficient communication between source and destination. The attacks in the wireless or Mobile AdHoc network scenarios are: DOS, Wormhole attack and Blackhole attacks, Sniffing, Sybil and so on.

Portable specially appointed systems will show up in situations where the hubs of the systems are missing and have next to zero physical assurance against altering. The hubs of portable specially appointed systems are consequently powerless to trade off. The systems are especially helpless against disavowal of administration (DOS) assaults propelled through bargained hubs or gatecrashers. This work proposed another DOS assault and its guard in specially appointed systems. The new DOS assault, called Ad Hoc Flooding Attack(AHFA), can bring about disavowal of administration when utilized against on-request steering conventions for portable specially appointed systems, for example, AODV, DSR. The gatecrasher communicates mass Route Request parcels to debilitate the correspondence data transmission and hub asset so the legitimate correspondence can't be kept.

II. OVERVIEW OF EXISTING APPROACH

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as Flooding, Blackhole, Sybil and so on. In Flooding or Denial of Service (DOS) attacks, a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called attacker node) can attract all packets by using forged Route Reply packet to falsely claim that “fake” shortest route to the destination and then discard these packets without forwarding them to the destination. In DOS attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. The malicious nodes are termed as affected/false/fake/abnormal Nodes in this case and there is no alternative mechanisms to solve the routing issues and avoid the attack possibilities while communication.

III. REQUIREMENT SPECIFICATION

System Requirements

Hardware Requirements

System	: Pentium IV 2.4 GHz
Hard Disk	: 40 GB
Ram	: 512 Mb

Software Requirements

Operating system	: Windows / Linux

Technology Used : NS2

IV. PROPOSED APPROACH & ALGORITHM

In the proposed approach, new mechanisms are introduced, which aims at detecting and preventing malicious nodes launching Flooding or Denial of Service attacks in Mobile AdHoc environment via the effective identification and removal of Fictitious/false Nodes in scenario. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait (RREQ-RREP) destination address to bait malicious nodes to send a reply message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.

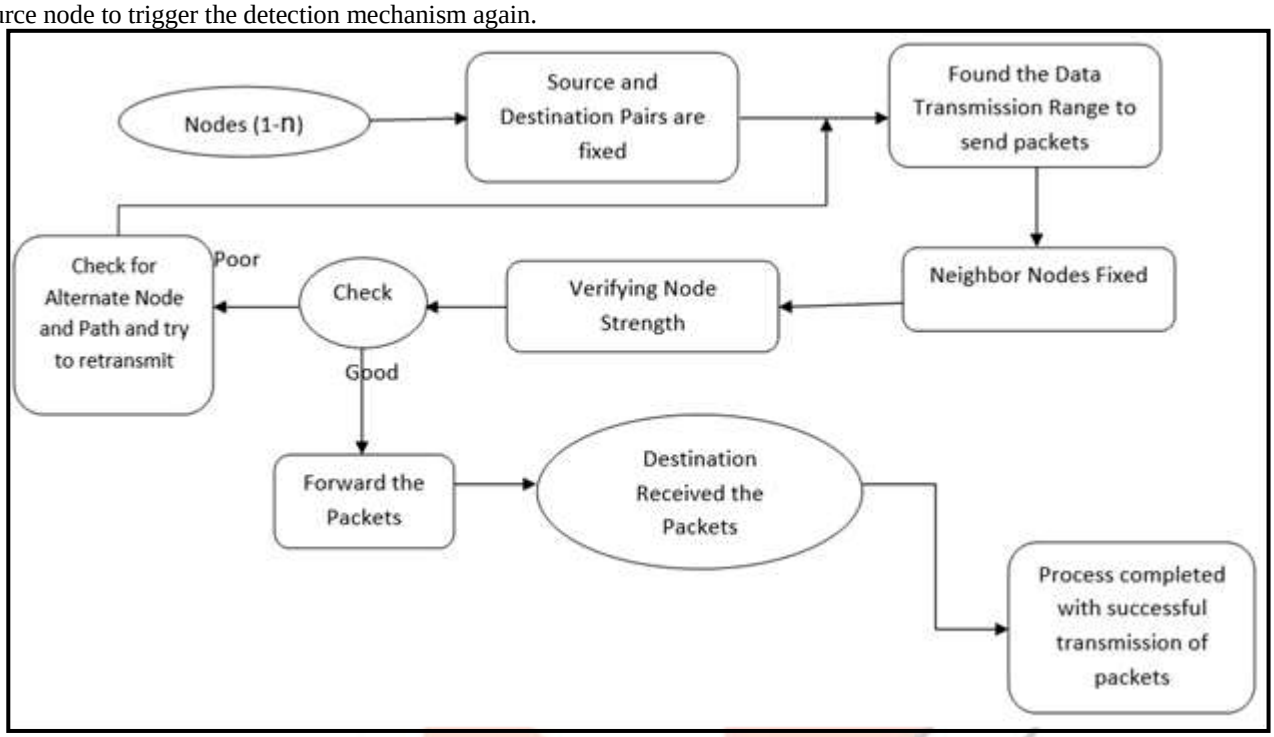


Fig.1. Proposed Framework

This system proposes a fault node recovery (FNR) algorithm for WSNs based on the grade diffusion algorithm combined with the genetic algorithm. The FNR algorithm creates the grade value, routing table, neighbor nodes, and payload value for each sensor node using the grade diffusion algorithm. In the FNR algorithm, the number of nonfunctioning sensor nodes is calculated during the wireless sensor network operation and the parameter based illustrations. In this approach we are using the Directed Diffusion Algorithm, which has the goal to reduce the data relay transmission counts for power management and with this algorithm we can show better results of Throughput as well as Delay management. In proposed approach we combine Grade Diffusion Algorithm with Genetic algorithm, which is used to select the Routing Criteria and Estimating the definition for Resolver Node

V. ALGORITHM

Step-1: input number of nodes between given range.

Example: “Enter No. of Nodes between 40 and 60 :” [n]

If not between 40 to 60

Then exit

Step-2: Select source node from given range.

Example: S1=n-20

“Enter the Source Node between 10 and (n-20) :” [src]

If not between 10 to (n-20)

Then exit

Step-3: Select destination node from given range.

Example: d1=src+5, d1x=src+2 , d2=src+10

If d2>n

D1=d1x

else

d2=n

“Enter the destination Node between d1 and d2 :” [dest]

If not between d1 and d2

Then exit

Step-4: find neighboring nodes [using node difference]

Example: node difference = dest-src

If node difference =1 then 1 neighboring node
If node difference =2 then 2 neighboring nodes
…
...
If node difference =20 then 20 neighboring nodes

Step-5: Starts selecting the Neighbor Node
Step-6: Checking the strength of neighboring node
Step-7: if good (> threshold) then forward to neighbor node
Step-8: if poor then check for another path
Step-9: sending of data routing request to neighbor node
Step-10: if Neighbor Nod does not Send Routing Response yet...
Step-11: if doesn't give response up to some defined time limit then neighbor Node marks Node as Fault Node..
Step-12: Resolver Node Starts Recovering the Neighbor Node.
Step-13: After recovery, transmission completed and packet reaches to destination with the help of all neighbouring nodes.

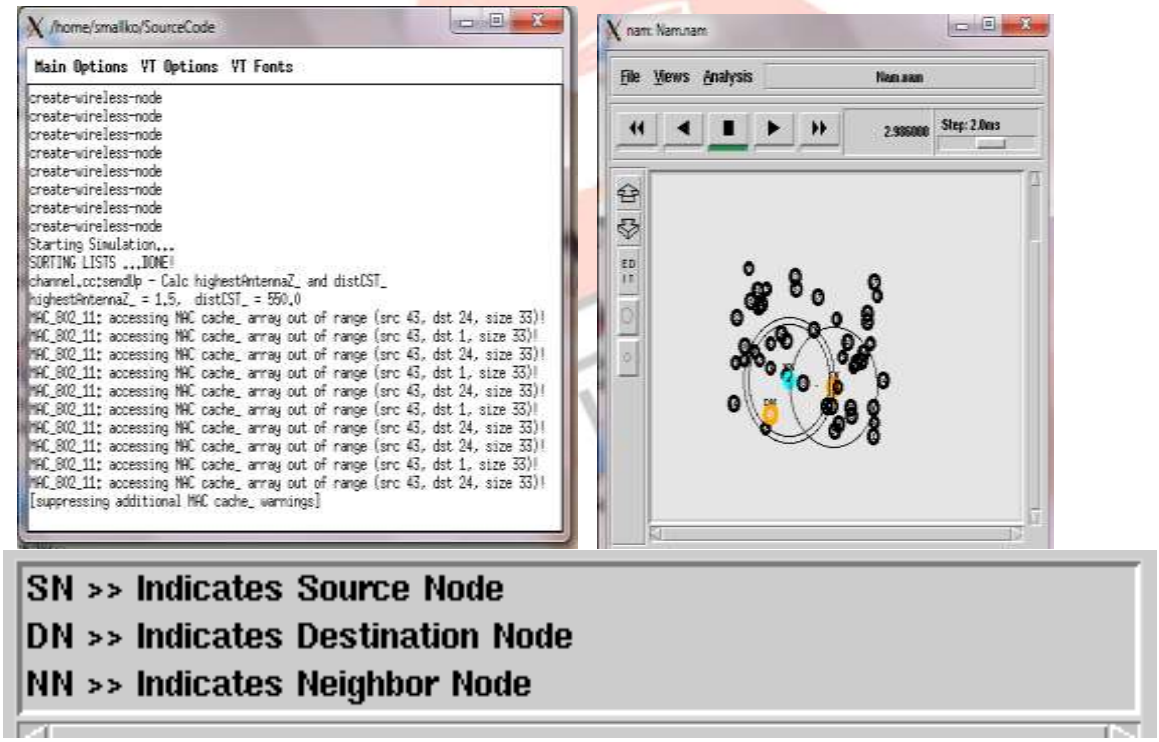
V IMPLEMENTATION & RESULTS

Step-1: We have pre define following parameters for execution of proposed flow.

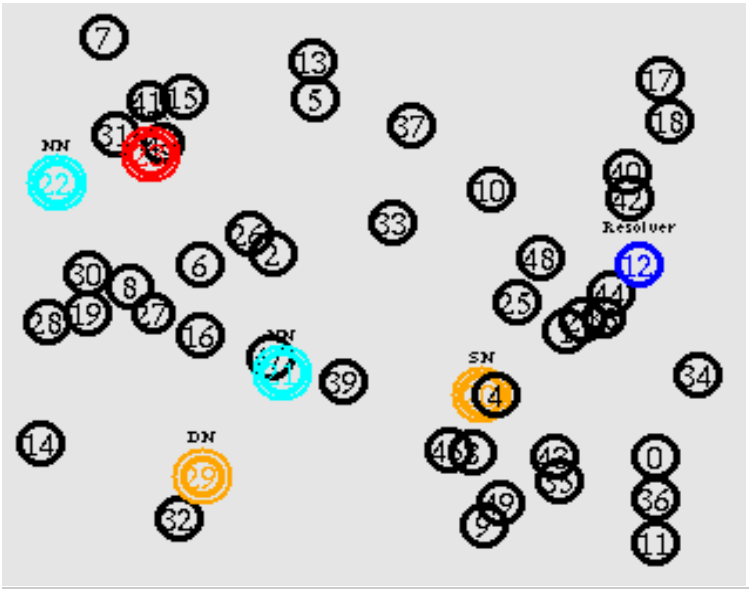
- No of nodes
- Source node
- Sink node
- Transmission packet size in bytes
- Individual node strength
- Packet transmission speed in bps
- Mobility speed
- Transmission range in meters.

Step-2 : Creation of node

Step-3 : Node Formulation



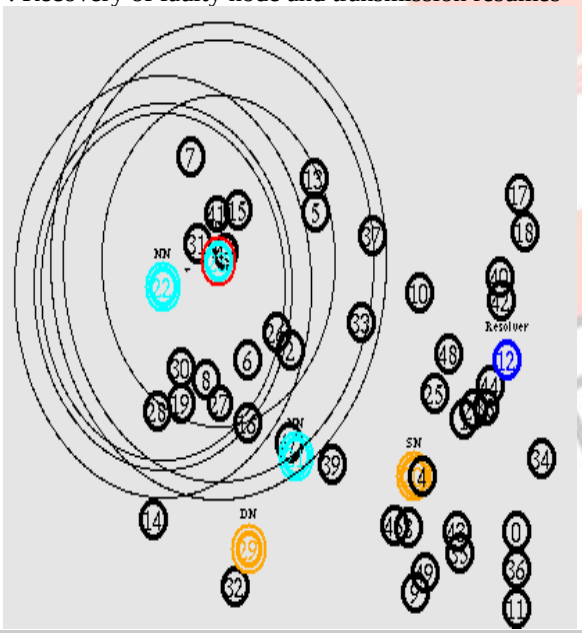
Step-4 : Detection of Faulty node 23 & working of Resolver node 12



Neighbor Node-22 Starts selecting the Neighbor Node-23 and Send Data Routing Request
Neighbor Node-23 does not Send Routing Response yet...
Neighbor Node-23 Failed to Send Routing Response...

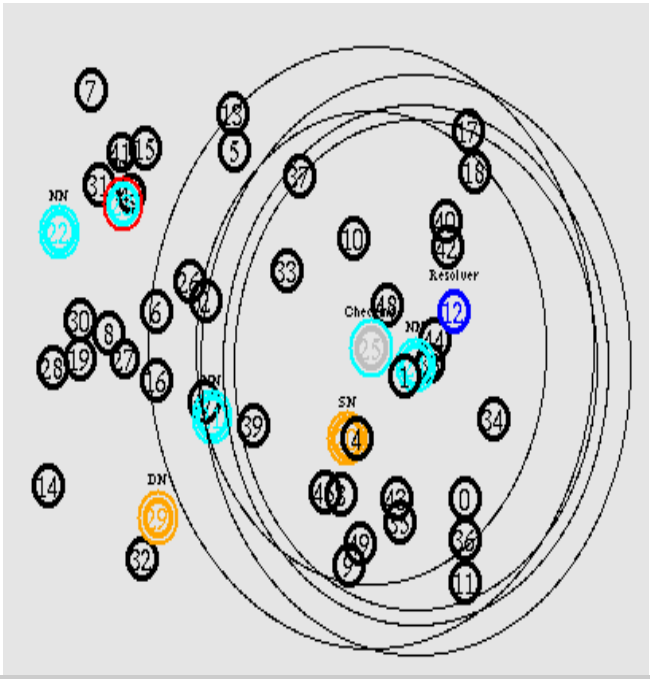
Neighbor Node-23 Failed to Send Routing Response...
Neighbor Node-22 marks Node-23 as Fault Node...
Resolver Node-12 Starts Recovering the Neighbor Node-23

Step-5 : Recovery of faulty node and transmission resumes



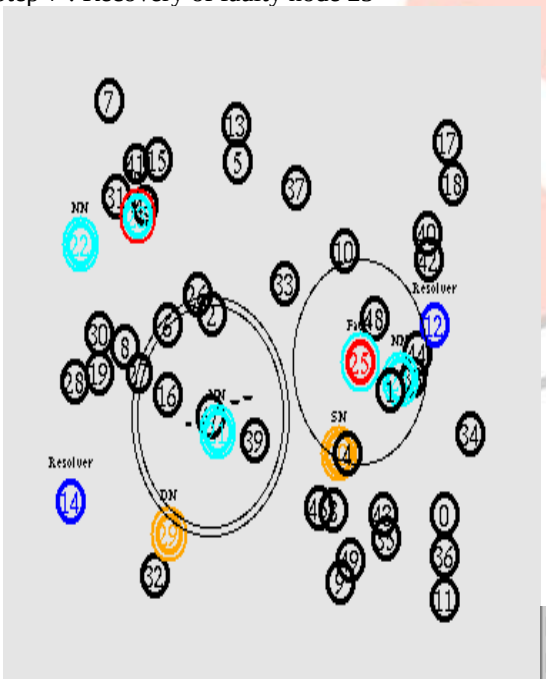
Resolver Node-12 Recovered Neighbor Node-23
Node-22 Starts Transmission with Neighbor Node-23

Step-6 : Further Transmissions and detection of another faulty node



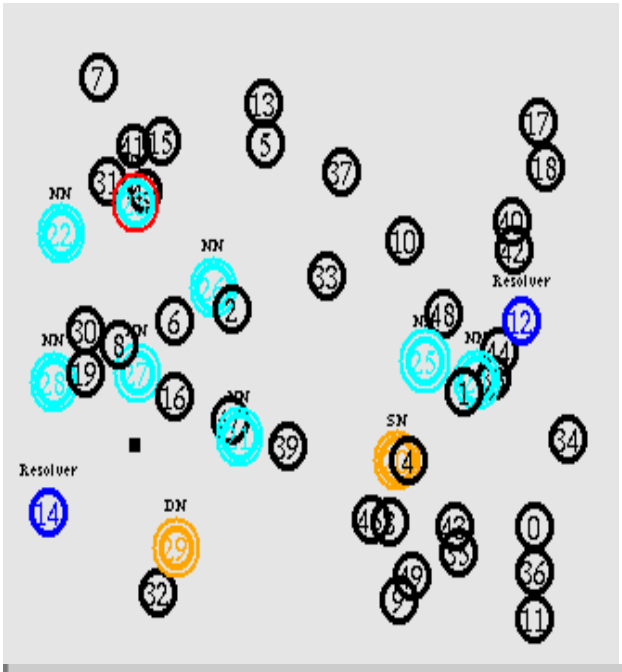
Neighbor Node-24 Starts selecting the Neighbor Node-25 and Send Data Routing Request
Neighbor Node-25 does not Send Routing Response yet...

Step-7 : Recovery of faulty node 25



Neighbor Node-24 marks Node-25 as Fault Node...
Resolver Node-14 Starts Recovering the Neighbor Node-25

Step-8: After recovery, transmission completed and packet reaches to destination 29 with the help of all neighbouring nodes.



Resolver Node-14 Recovered Neighbor Node-25

VI ANALYSIS

Fig.2 Graph of energy consumption level ,Performance of average delay vs speed, Life time analysis, throughput analysis

REFERENCES

[1] Bahaddur, Indira, C. L. Triveni, and P. C. Srikanth. "Novel Defense mechanism against data flooding attacks in ad hoc network." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.

[2] Chouhan, Neetu Singh, and Shweta Yadav. "Flooding attacks prevention in MANET." International Journal of Computer Technology and Electronics Engineering (IJCTEE) 1.3 (2011): 2011.

[3] Yi, Ping, et al. "Performance analysis of mobile ad hoc networks under flooding attacks." Journal of Systems Engineering and Electronics 22.2 (2011): 334-339.

[4] Singh, Virendra Pal, Sweta Jain, and Jyoti Singhai. "Hello flood attack and its countermeasures in wireless sensor networks." IJCSI International Journal of Computer Science Issues 7.11 (2010): 23-27.

[5] Shandilya, Shishir K., and Sunita Sahu. "A trust based security scheme for RREQ flooding attack in MANET." International journal of computer applications 5.12 (2010): 4-8.

[6] Performance of AOMDV Routing Protocol Under Rushing and Flooding Attacks in MANET ,2015

[7] SYN FLOODING ATTACK – IDENTIFICATION AND ANALYSIS , 2014

[8] Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol , 2014.

[9] Flooding Attacks Prevention in MANET , 2013

[10] Flooding Attacks Detection in MANETs , 2015

[11] A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks , 2015

[12] A survey defense mechanisms against distributed denial pf service flooding attacks , IEEE 2013.

[13] A Literature Review of Security Attack in Mobile Ad-hoc Networks Nov. 2010.

[14] An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in MANET , 2013.

[15] Detection of Malicious Attack in MANET A Behavioral Approach , 2013.

[16] J. A. Carballido, I. Ponzoni, and N. B. Brignole, "CGD-GA: A graphbased genetic algorithm for sensor network design," Inf. Sci., vol. 177, no. 22, pp. 5091–5102, 2007.

[17] F. C. Chang and H. C. Huang, "A refactoring method for cache-efficient swarm intelligence algorithms," Inf. Sci., vol. 192, no. 1, pp. 39–49, Jun. 2012.

[18] S. Corson and J. Macker, Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. New York, NY, USA: ACM, 1999.

[19] M. Gen and R. Cheng, Genetic Algorithms and Engineering Design. New York, NY, USA: Wiley, 1997.

[20] Z. He, B. S. Lee, and X. S. Wang, "Aggregation in sensor networks with a user-provided quality of service goal," Inf. Sci., vol. 178, no. 9, pp. 2128–2149, 2008.

[21] J. H. Ho, H. C. Shih, B. Y. Liao, and S. C. Chu, "A ladder diffusion algorithm using ant colony optimization for wireless sensor networks," Inf. Sci., vol. 192, pp. 204–212, Jun. 2012.

[22] J. H. Ho, H. C. Shih, B. Y. Liao, and J. S. Pan, "Grade diffusion algorithm," in Proc. 2nd Int. Conf. Eng. Technol. Innov., 2012, pp. 2064–2068.

[23] T. P. Hong and C. H. Wu, "An improved weighted clustering algorithm for determination of application nodes in heterogeneous sensor networks," J. Inf. Hiding Multimedia Signal Process., vol. 2, no. 2, pp. 173–184, 2011.

[24] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 2–16, Feb. 2003.

[25] W. H. Liao, Y. Kao, and C. M. Fan, "Data aggregation in wireless sensor networks using ant colony algorithm," J. Netw. Comput. Appl., vol. 31, no. 4, pp. 387–401, 2008.

[26] T. H. Liu, S. C. Yi, and X. W. Wang, "A fault management protocol for low-energy and efficient wireless sensor networks," J. Inf. Hiding Multimedia Signal Process., vol. 4, no. 1, pp. 34–45, 2013.