ISSN: 0976-3104

SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)

ARTICLE OPEN ACCESS

IMPROVING EFFICIENCY OF SELFISH NODE DETECTION IN AD-HOC NETWORK USING COLLABORATIVE CONTACT BASED WATCHDOG

Meenakshi P*, V. Jayashreeja, D. Gayathri, C. Sowmya

Vel Tech, Dr. RangarajanDr.Sakunthala Engineering College, INDIA

ABSTRACT

In ad-hoc networks, there are some nodes which refuse to co-operate with network in transferring the data. Such nodes behave in a selfish manner and hence called selfish nodes. Due to the presence of selfish nodes, the problem of false positive and false negative occurs. Therefore detecting those nodes is essential for the overall performance of the network. For detecting such nodes and reducing the positive and negative detections, we introduce a COCOWA model that would launch the collaborative contact-based watchdog. It detects by collecting the forwarding history evidence from its upstream and downstream nodes. To further improve the performance of the proposed collaborative inspection scheme, a reputation system is introduced, in which the inspection probability could vary along with the target node's reputation. Under this system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability.Downstream nodes. To further improve the performance of the proposed collaborative inspection scheme, a reputation system is introduced, in which the inspection probability could vary along with the target node's reputation. Under this system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability.

Published on: 08th– August-2016

KEY WORDS

AD-HOC network, selfish node detection

***Corresponding author: Email:** minuraj11@gmail.com; **Tel:** +91 9710432387

INTRODUCTION

The fundamental task of the nodes in the network is to transfer the data from source to destination successfully. Mobile ad-hoc networks constitute the mobile nodes which move with a certain mobility. In mobile ad-hoc networks, the mobile nodes voluntarily cooperate in order to work properly. This is a cost-intensive activity and some nodes can refuse to cooperate leading to selfish node behavior. The above situation can lead to the decrease in network performance. The watchdog is a well-known mechanism to detect selfish nodes, but they can fail, generating false positive and false negative that can induce to wrong operations. Moreover relaying on local watchdogs alone can leave to poor performance when detecting selfish nodes in term of precision and speed.This is especially important on networks with sporadic contacts, such as Delay Tolerant Networks (DTNs) where sometimes watchdogs lack of enough time or information to detect the selfish nodes. Thus we propose Collaborative Contact-based watchdog (COCOWA) as a collaborative approach based on thediffusion of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. Selfishness means that some nodes refuse to forward other nodes 'packets to save their own resources. InDTNs,selfish nodes can seriously degrades the performance of packet transmission. In a survey, the number of packet losses is increased by 500 percent when the selfish node ratio increases from 0 to 40%.Another problem is the presence of colluding or malicious nodes. Malicious node intentionally disturbs the correct behavior of the network, so the detection process is necessary for the proper performance of the network.

EXISTING SYSTEM

The local watchdog does not evaluate the effect of false positives, false negatives and malicious nodes. For example, the approach only transmits positive detections. The problem is that if a false positive is generated it can spread this wrong information very quickly on the network, isolating nodes that are not selfish. Therefore, an approach that includes the diffusion of negative detections as well becomes necessary. Another problem is the impact of colluding or malicious nodes. Although a reputation system can be useful to mitigate the effect of malicious nodes, it clearly depends on how are combined local and global ratings, as shown in this paper. Another implementation issue is the high imposed overhead due to the flooding process in order to achieve a fast diffusion of the information

Problem Definition

- Attack detection process is not satisfied.
- High communication cost overhead due to the data transmission from source to destination.
- The data transmission process takes much time.

PROPOSED SYSTEM

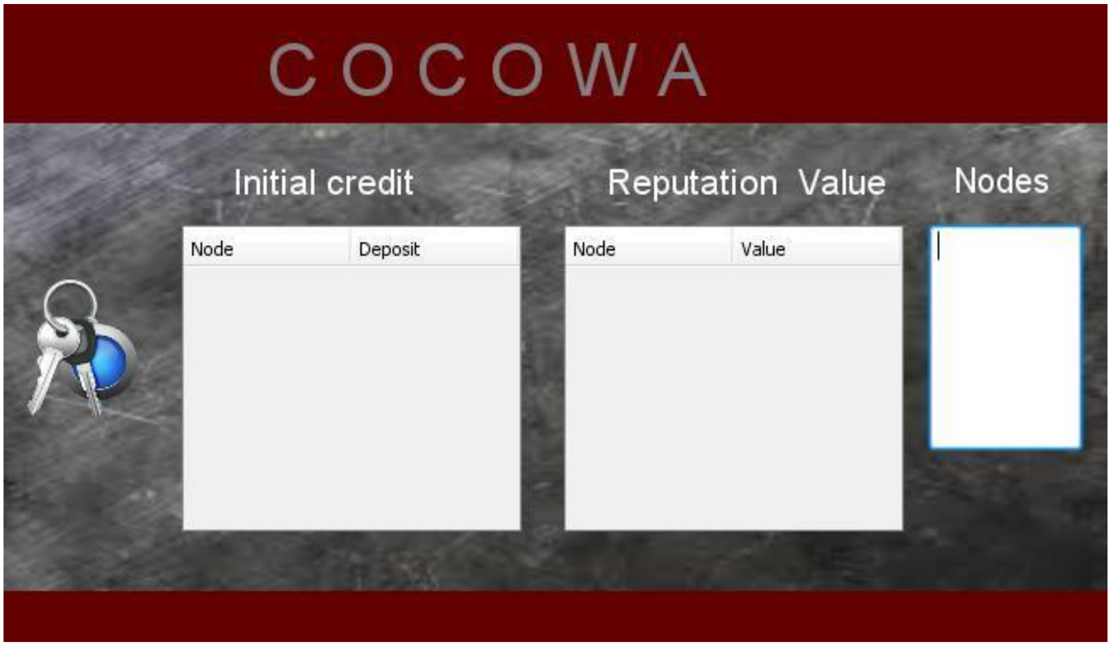
This paper proposes CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, false negatives and malicious nodes. CoCoWa technique is used to detect Sybil attack, black whole attack and redirect attack. Nodes is attacked by (I)Sybil attack, it will forward the data but it won't acknowledge to the source, it won't forward the data but it will acknowledge to the source.(II)Black whole attack, it will interprets the data.(III) Redirect attack is to forward the data to source. CoCoWa can reduce the overall detection time with respect to the original detection time when collaboration scheme is not issued, with a reduced overhead (message cost).

SNAPSHOTS

THE HOME SCREEN

A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes In Cooperative MANET

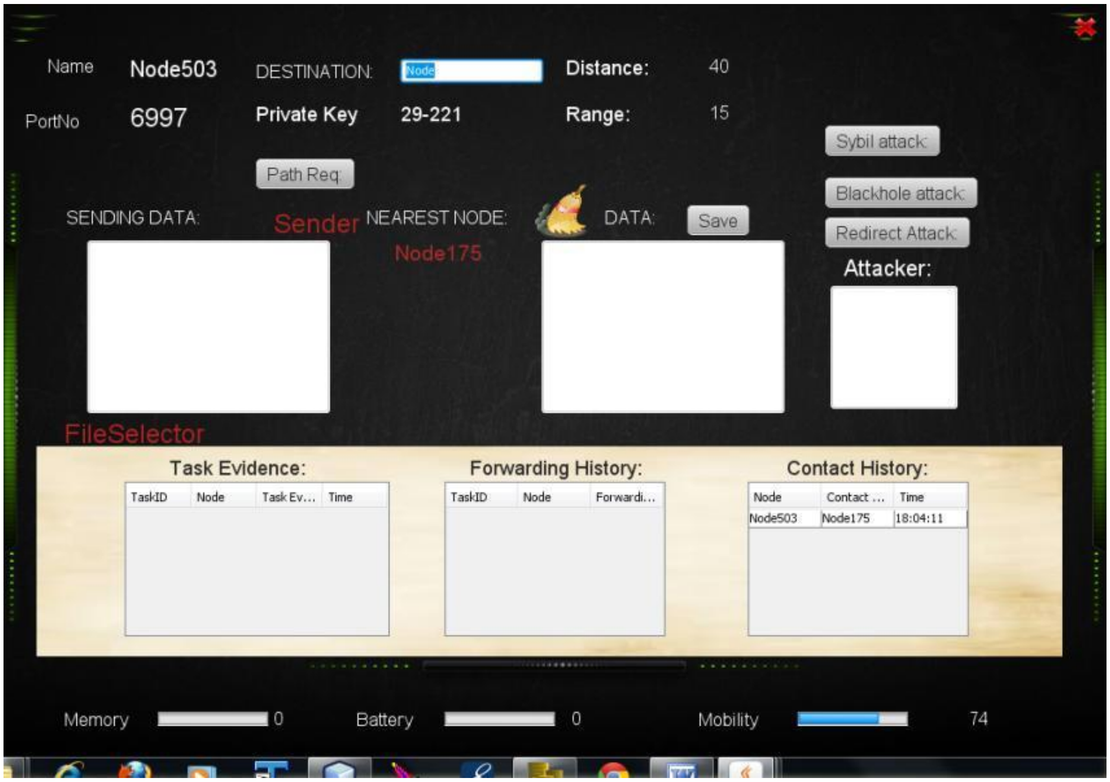
COCOWA



Node	Deposit

Node	Value

CREATION OF NODES



Name Node503 DESTINATION: Node Distance: 40

PortNo 6997 Private Key 29-221 Range: 15

SENDING DATA: Sender NEAREST NODE: Node175 DATA: Attacker:

Task Evidence:

TaskID	Node	Task Ev...	Time

Forwarding History:

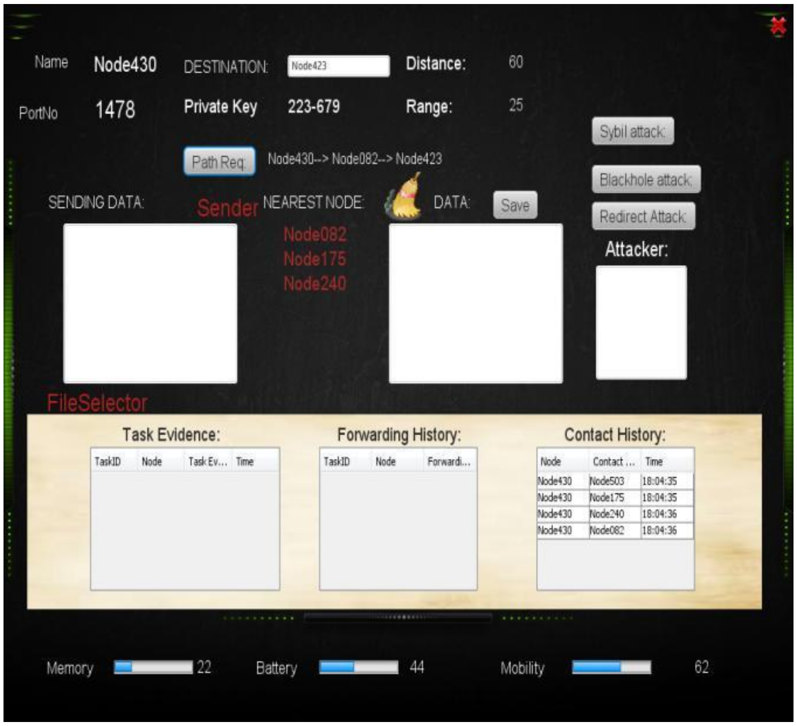
TaskID	Node	Forwardi...

Contact History:

Node	Contact ...	Time
Node503	Node175	18:04:11

Memory 0 Battery 0 Mobility 74

PATH REQUEST



Name Node430 DESTINATION: Node423 Distance: 60

PortNo 1478 Private Key 223-679 Range: 25

Node430--> Node082--> Node423

SENDING DATA: Sender NEAREST NODE: DATA: Attacker:

Node082
Node175
Node240

Task Evidence:

TaskID	Node	Task Ev...	Time

Forwarding History:

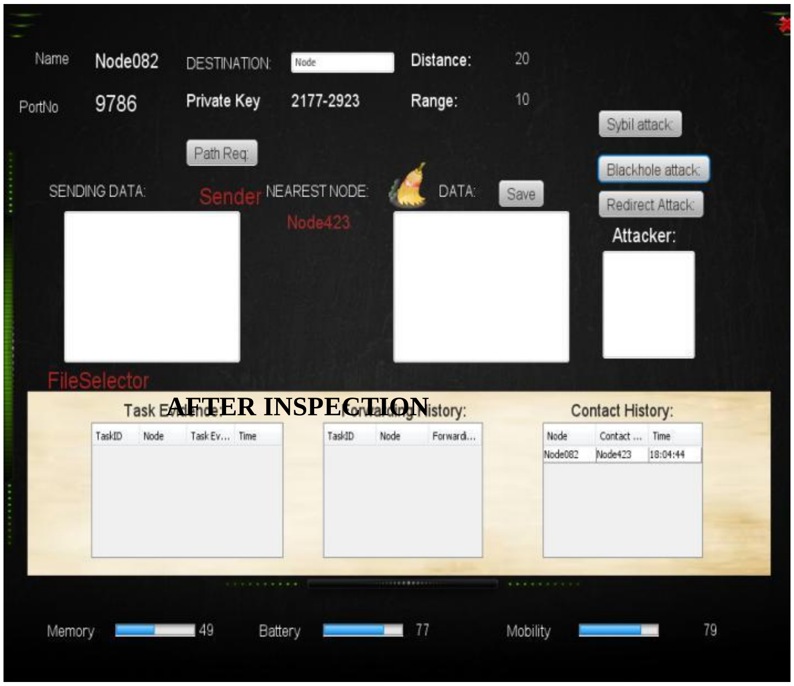
TaskID	Node	Forwardi...

Contact History:

Node	Contact ...	Time
Node430	Node503	18:04:35
Node430	Node175	18:04:35
Node430	Node240	18:04:36
Node430	Node082	18:04:36

Memory 22 Battery 44 Mobility 62

BLACK HOLE ATTACK



Name Node082 DESTINATION: Node Distance: 20

PortNo 9786 Private Key 2177-2923 Range: 10

SENDING DATA: Sender NEAREST NODE: DATA: Attacker:

Node423

AFTER INSPECTION

Task Evidence:

TaskID	Node	Task Ev...	Time

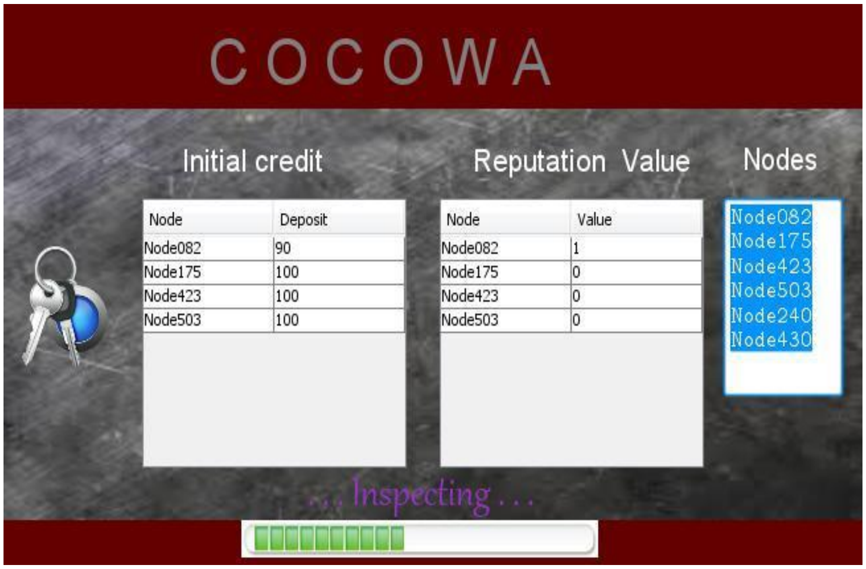
Forwarding History:

TaskID	Node	Forwardi...

Contact History:

Node	Contact ...	Time
Node082	Node423	18:04:44

Memory 49 Battery 77 Mobility 79



Node	Deposit
Node082	90
Node175	100
Node423	100
Node503	100

Node	Value
Node082	1
Node175	0
Node423	0
Node503	0

Node082
Node175
Node423
Node503
Node240
Node430

CONCLUSION

Thus we design, to reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively for secure MANET routing.

CONFLICT OF INTEREST

Authors declare no conflict of interest.

ACKNOWLEDGEMENT

None.

FINANCIAL DISCLOSURE

No financial support was received to carry out this project.

REFERENCES

[1] S Abbas, M Merabti, D Llewellyn-Jones, and K.Kifayat.[2013]Lightweight sybil attack detection in manets, *IEEE Syst J*, 7(2): 236–248

[2] S Bansal and M. Baker.[2003.] Observation-based cooperation enforcement in ad hoc networks, arXiv:cs.NI/0307012,

[3] S Buchegger and J.-Y.Le Boudee, Self-policing mobile ad hoc networks by reputation systems, *IEEE Commun.Mag*, 43.