IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 5, May 2018

Defending the Data from Selfish Node and Malicious Node in MANETs

J.Saranya[1], Mr. R.Arun Kumar M.E.,[2]

United institute of Technology, Computer Science and Engineering, Coimbatore[1]

Assistant Professor, United Institute of Technology, Computer Science and Engineering, Coimbatore[2]

Abstract: Mobile Ad-hoc Networks (MANETs) assume that mobile nodes voluntary cooperate in order to work properly. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Thus, the overall network performance could be seriously affected. The use of watchdogs is a well-known mechanism to detect selfish nodes. However, the detection process performed by watchdogs can fail, generating false positives and false negatives that can induce to wrong operations. Moreover, relying on local watchdogs alone can lead 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 watchdog's 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 the diffusion of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. As shown in the paper, this collaborative approach reduces the time and increases the precision when detecting selfish nodes.

Keywords: Wireless networks, MANETs, opportunistic and delay tolerant networks, selfish nodes, performance evaluation.

I. INTRODUCTION

COOPERATIVE networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as vehicular ad hoc networks (VANETs) or mobile social networks. Two of the basic technologies that are considered as the core for these types of networks are mobile ad-hoc networks (MANETs) and opportunistic and delay tolerant networks (DTNs). The cooperation on these networks is usually contact- based. Mobile nodes can directly communicate with each other if a contact occurs (that is, if they are within communication range). Supporting this cooperation is a cost intensive activity for mobile nodes. Thus, in the real world, nodes could have a selfish behavior, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources. The literature provides two main strategies to deal with selfish behavior: a) motivation or incentive based approaches, and b) detection and exclusion.

The first approach, tries to motivate nodes to actively participate in the forwarding activities. These approaches are usually based on virtual currency and/or game theory models. The detection and exclusion approach is a straight-forward way to cope with selfish nodes and several solutions have been presented. In CoCoWa, we do not attempt to implement any strategy to exclude selfish nodes or to incentivize their participation; instead, we focus on the detection of selfish nodes.

II. RELATED WORKS

Mobility is often a problem for providing security services in ad hoc networks. In this paper, [1] we show that mobility can be used to enhance security. Specifically, we show that nodes that passively monitor traffic in the network can detect Sybil attacker that uses a number of network identities simultaneously. We show through simulation that this detection can be done by a single node, or that multiple trusted nodes can join to improve the accuracy of detection .We then show that although the detection mechanism will falsely identify groups of nodes traveling together as a Sybil attacker, we can extend the protocol to monitor collisions at the MAC level to differentiate between a single attacker spoofing many addresses and a group of nodes traveling in close proximity.

Ad hoc networks rely on the cooperation of the nodes participating in the network to forward packets for each other. [2] A node may decide not to cooperate to save its resources while still using the network to relay its traffic. If too many nodes exhibit this behavior, network performance grades and cooperating nodes may find themselves unfairly loaded. Most previous efforts to counter this behavior have relied on further cooperation between nodes to exchange reputation

DOI 10.17148/IJARCCE.2018.7534

information about other nodes. If a node observes another node not participating correctly, it reports this observation to other nodes who then take action to avoid being affected and potentially punish the bad node by refusing to forward its traffic. Unfortunately, such second-hand reputation information is subject to false accusations and requires maintaining trust relationships with other nodes.

This paper proposes a combination of an Intrusion Detection System [3] with a routing protocol to strengthen the defense of a Mobile Adhoc Network. Our system is Socially Inspired, since we use the new paradigm of Reputation inherited from human behavior. The proposed IDS also has a unique characteristic of being Semi-distributed, since it neither distributes its Observation results globally nor keeps them entirely locally; however, managing to communicate this vital information without accretion of the network traffic. This innovative approach also avoids void assumptions and complex calculations for calculating and maintaining trust values used to estimate the reliability of other nodes' observations. A robust Path Manager and Monitor system and Redemption and Fading concepts are other salient features of this design. The design has shown to outperform normal DSR in terms of Packet Delivery Ratio and Routing Overhead even when up to half of nodes in the network behave as malicious.

Ad hoc wireless networks [4] have emerged as one of the key growth areas for wireless networking and computing technology. Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected.

Most of the routing protocols in wireless ad hoc networks, such as DSR, assume nodes are trust worthy and cooperative. One of the major factors effecting the ad ho communication is the misbehaving of nodes. Although an efficient power management scheme is applied to an ad hoc network, a misbehaving node may result in the improper routing of packet which may extend to the complete collapsing of the network also. Existing approaches such as economic incentives or secure routing by cryptographic means alleviate the problem to some extend with limitations.

III. PROPOSED MEHODOLOGY

This paper introduces Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs.

This way, nodes have second hand information about the selfish nodes in the network. The goal of our approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives. Although some of the aforementioned introduced some degree of collaboration on their watchdog schemes, the diffusion is very costly since they are based on periodic message dissemination.

3.1 METHODOLOGIES

A selfish node usually denies packet forwarding in order to save its own resources. This behavior implies that a selfish node neither participates in routing nor relays data packets. A common technique to detect this selfish behavior is network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmitted and received by its neighbors in order to detect anomalies, such as the ratio between packets received to packets being re-transmitted .

SENDER

- AUTHENTICATION
- CHOOSE DESTINATION
- SHARE PACKET
- REPORTS

WATCHDOG

- UPDATE INFORMATION
- MONITOR NODE
- ROUTE INFORMATION

RECEIVER

- AUTHENTICATION
- VIEW ACKNOWLEDGEMENT
- RECEIVE PACKETS

ADMIN

- AUTHENTICATION
- MONITORING NETWORK
- PERFORMANCE EVALUATION
- REPORTS

DOI 10.17148/IJARCCE.2018.7534

3.2 MODULE DESCRIPTION & DIAGRAMS

SENDER

Authentication

The user has to give exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

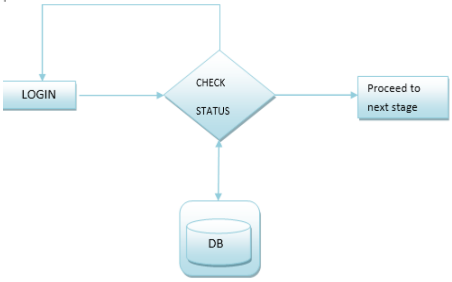


Fig: 3.2.1 Sender page

Choose destination

In this module sender has to select the receiver node from the network. MANET has N- Number of mobile node in the network. If any node wants to send a packet to the other node then the transfer node act as sender the destination node is called as receiver.

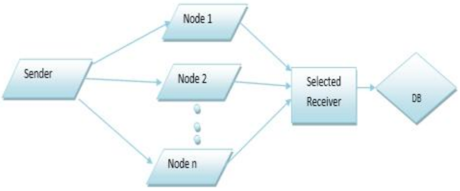


Fig: 3.2.2 Choosing destination

Share packet

After the successful completion of the login and the node receiver selection Sender has to decide to send a packet into the network. Before that then could address the intermediate node for the File sharing and then they will send into the Mobile network.

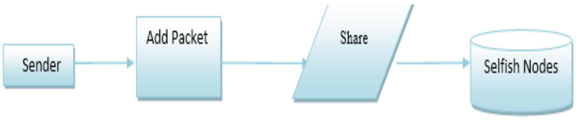


Fig: 3.2.3 Sharing packet

Reports

The Admin generates the reports based on the Performance the values which is obtained from the analysis module. It could be easy to understand the overall quality of the web services

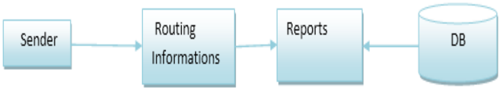


Fig: 3.2.4 Report analysis

WATCHDOG

Update information

In this module dynamically the information has been updated. It contains the sender information's and intermediate node information's that has the routing information of all the nodes in the network

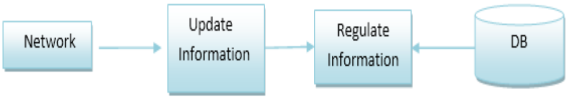


Fig: 3.2.5 Information updating

DOI 10.17148/IJARCCE.2018.7534

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 5, May 2018

Monitor node

In this scheme regulator just monitor the service which has been sold by the seller in the mobile network. Just they can figure out how many intermediate has been get the packet and they could see over all list of the selfish node in the MANET.

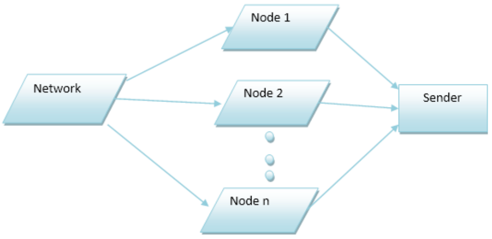


Fig: 3.2.6 Monitor node

Route information

In this module dynamically the information has been updated. It contains the sender information's and intermediate node information's that has the routing information of all the nodes in the network

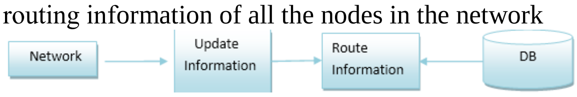


Fig: 3.2.7 Route information

RECEIVER

Authentication

The user has to give exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

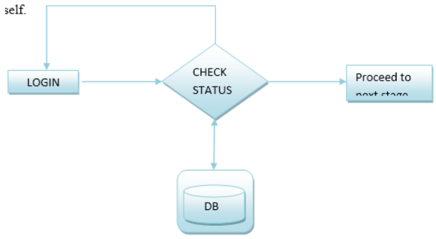


Fig: 3.2.8 Receiver page

View acknowledgement

In this module the receiver has to see the total number of file is going to receive that has been intimated before the packet receiving.

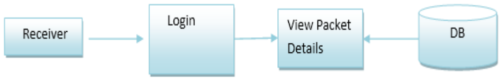


Fig: 3.2.9 view acknowledgement

Receive packets

In this module receiver has to receive the files through the intermediate node. Watchdog always watches the source information. If any node not able to route the received packet within the particular range time then that node is called as selfish node and it spread a negative message to all the nods in the entire network.

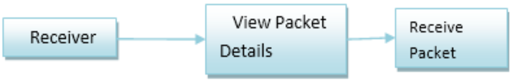


Fig: 3.2.10 Receiver packets

ADMIN

Authentication

The user has to give exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself

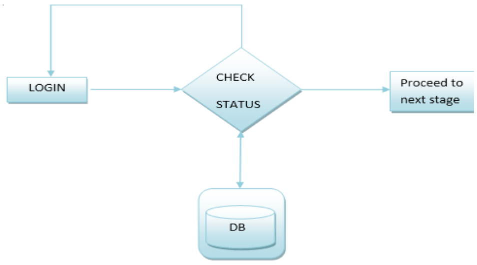


Fig: 3.2.11 Admin page

Monitoring network

In this scheme regulator just monitor the service which has been sold by the seller in the mobile network. Just they can figure out how many intermediate has been get the packet and they could see over all list of the selfish node in the MANET.

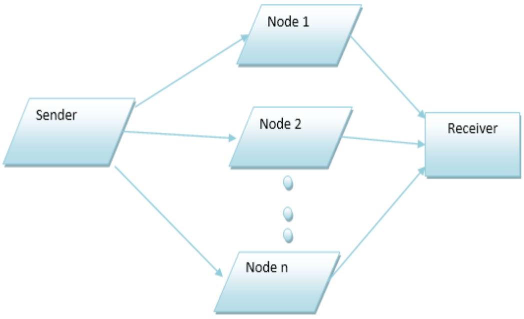


Fig: 3.2.12 Monitoring network

Performance evaluation

In this module the entire node performance will be evaluated here. This might easily identify the each and every node performance in the network. The report is generated in the form of graphical chart this could show overall evaluation.

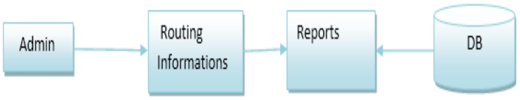
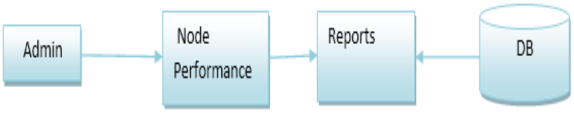


Fig : 3.2.13 Performance evaluation

Reports

The Admin generates the reports based on the Performance the values which is obtained from the analysis module. It could be easy to understand the overall quality of the web services



TECHNIQUE USED OR ALGORITHM USED

Collaborative Contact-based Watchdog (CoCoWa)

A selfish node usually denies packet forwarding in order to save its own resources. This behavior implies that a selfish node neither participates in routing nor relays data packets. A common technique to detect this selfish behavior is network monitoring using local watchdogs.

A node's watchdog consists on overhearing the packets transmitted and received by its neighbors in order to detect anomalies, such as the ratio between packets received to packets being re- transmitted.

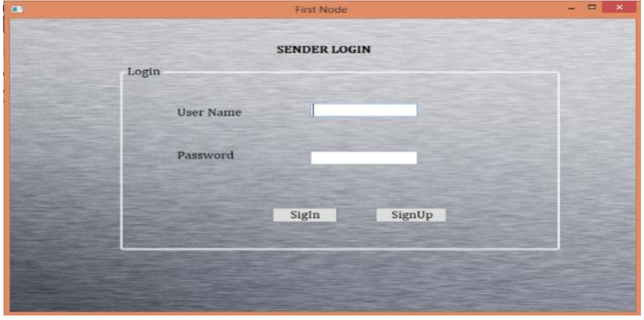
DOI 10.17148/IJARCCE.2018.7534

By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly (or not).

IV. RESULT AND DISCUSSION

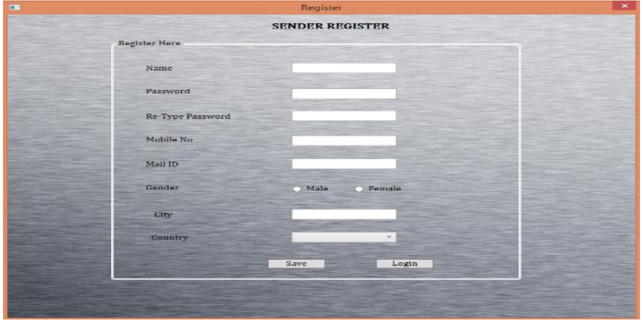
VARIOUS SNAPSHOTS

Sender Login Page:



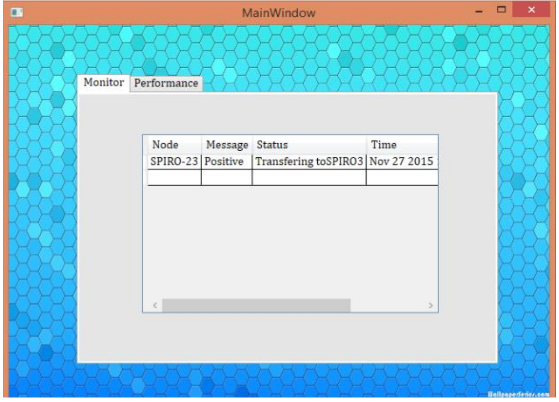
The above fig shows the design for seller login page of our project.
Input: Provide username and password to get permission for access.
Output: Became authenticated person to request and process the request.

Registration Page:



The above fig shows the design of sender Register form. Then Afteruser has to login using Id and password.

Update:

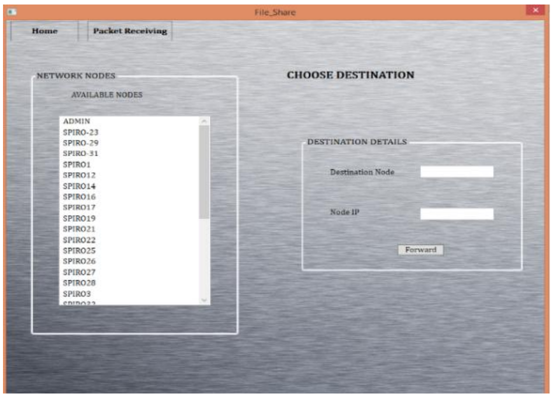


Node	Message	Status	Time
SPIRO-23	Positive	Transfering toSPIRO3	Nov 27 2015

The above fig shows the design of WATCHDOG interface
Input: File share information has stored in the database
Output: The stored information has been viewed in the grid

DOI 10.17148/IJARCCE.2018.7534

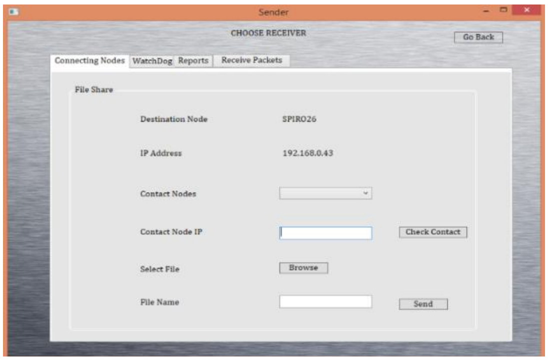
Choose receiver:



ADMIN
SPIRO-23
SPIRO-29
SPIRO-31
SPIRO1
SPIRO12
SPIRO14
SPIRO16
SPIRO17
SPIRO19
SPIRO21
SPIRO22
SPIRO25
SPIRO26
SPIRO27
SPIRO28
SPIRO3

The above fig :8.2.4shows the receiver list.

Connect Node:

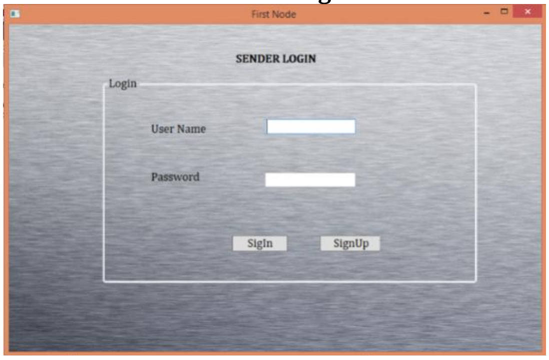


Destination Node SPIRO26

IP Address 192.168.0.43

Above Fig shows the whether the node is in the communication range or not.

Receiver Login:



The above fig shows the design for Receiver login page of our project.
Input: Regulator username and password to get permission for access.
Output: Became authenticated person to request and process the request.

Packet Request:

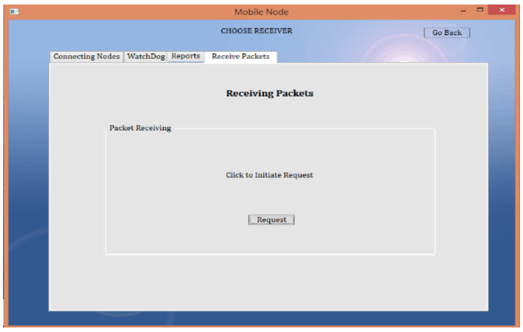
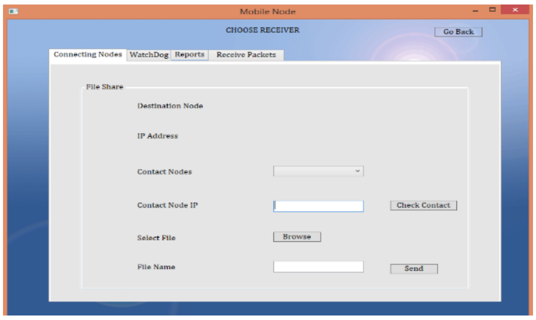


Fig: shows the design of file request.

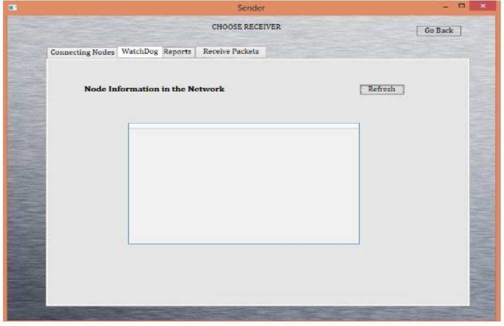
DOI 10.17148/IJARCCE.2018.7534

File Retrieve:



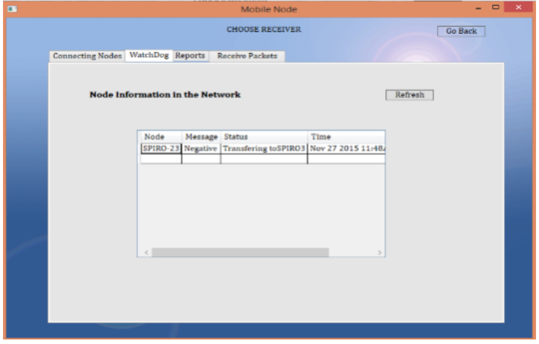
The above figshows the design of File receiving
Input: Receiver has to connect the device to the network.
Output: The result will be updated in the watchdog interface

Sender Watch Dog:



The above figshows the design of packet information in watch dog

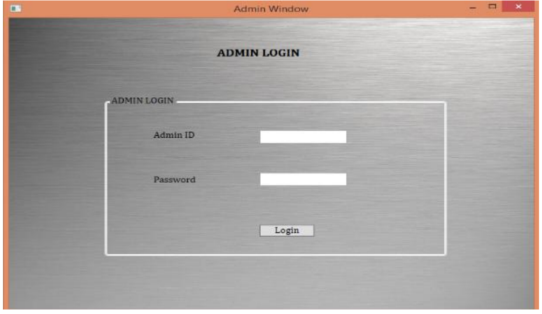
Sender Watch Dog:



Node	Message	Status	Time
SPIRO-23	Negative	Transfering toSPIRO3	Nov 27 2015 11:48/

The above fig shows the design of packet information in watch dog

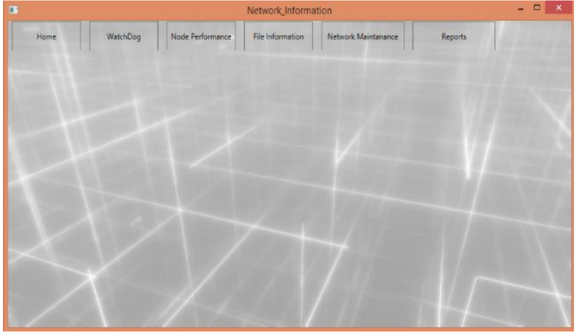
Admin Login:



The above figshows the design of Admin Login Form

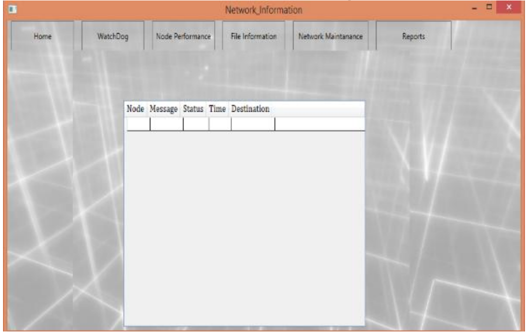
DOI 10.17148/IJARCCE.2018.7534

Admin Page:



This figure shows the admin Form layout

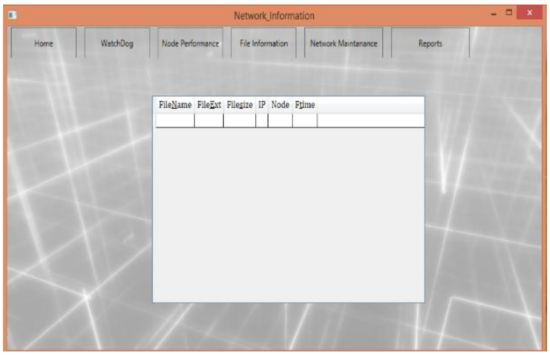
Admin Watch dog:



Node	Message	Status	Time	Destination

The above fig shows the design for watchdog dashboard.

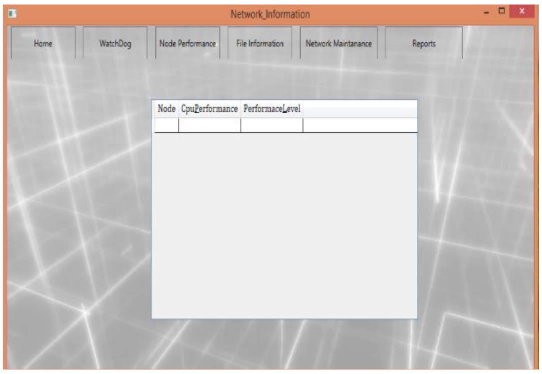
File Information:



FileName	FileExt	Filesize	IP	Node	Ftime

The above fig shows the design of File status information.

Network Performance:



Node	CpuPerformance	PerformaceLevel

This figure shows the network performance information.

DOI 10.17148/IJARCCE.2018.7534

V. CONCLUSION AND FUTURE WORK

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 is based on the diffusion of the known positive and negative detections. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections. Analytical and experimental results show that CoCoWa can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost).

REFERENCES

[1] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat,“Lightweight sybil attack detection in manets,” IEEE Syst. J.,vol. 7, no. 2, pp. 236–248, Jun. 2013.

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

[3] S. Buchegger and J.-Y.LeBoudee, “Self-policing mobile ad hoc networks by reputation systems,” IEEE Commun. Mag., vol. 43,no. 7, pp. 101–107, Jul. 2005.

[4] L. Buttyan and J.-P. Hubaux, “Enforcing service availability in mobile ad-hoc WANs,” in Proc. 1st Annu. Workshop Mobile Ad HocNetw. Comput., 2000, pp. 87–96.

[5] L. Buttyan and J.-P.Hubaux, “Stimulating cooperation in self organizing mobile ad hoc networks,” Mobile Netw. Appl., vol. 8,pp. 579–592, 2003.

[6] H. Cai and D. Y. Eun, “Crossing over the bounded domain: From exponential to power-law intermeeting time in mobile ad hoc networks,” IEEE/ACM Trans. Netw., vol. 17, no. 5, pp. 1578–1591,Oct. 2009.

[7] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott,“Impact of human mobility on opportunistic forwarding algorithms,”IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606– 620,Jun. 2007.

[8] J. R. Douceur, “The sybil attack,” in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[9] S. Eidenbenz, G. Resta, and P. Santi, “The COMMIT protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes,” IEEE Trans. Mobile Comput., vol. 7, no. 1,pp. 19–33, Jan. 2008.

[10] W. Gao, Q. Li, B. Zhao, and G. Cao, “Multicasting in delay tolerant networks: A social network perspective,” in Proc. 10th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2009, pp. 299–308.

DOI 10.17148/IJARCCE.2018.7534