IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-7 E-ISSN: 2347-2693

Selfish Node Detection in Wireless Networks

D. Nivetha[1*], D. Karthika[2]

[1*]Department of ECS, ARJ College of Engineering and Technology, Edayarnatham, India
[2]Department of ECS, ARJ College of Engineering and Technology, Edayarnatham, India

**Corresponding Author: dnivepenk@gmail.com*

Available online at: www.ijcseonline.org

Received: 22/Jun/2017, Revised: 06/Jul/2017, Accepted: 18/Jul/2017, Published: 30/Jul/2017

Abstract— Mobile ad-hoc networks (MANETs) relies on upon network participation plans to work legitimately. It expects that mobile node deliberate participate so as to work appropriately. By and by, if nodes have a selfish conduct and are unwilling to participate, the general network execution could be genuinely degraded. The proposed framework builds up a homomorphic straight Authenticator based upon examining design that enables the identifier to confirm the honesty of the bundle misfortune data detailed with nodes. In this manner, by recognizing the correlations between lost bundles, one can choose whether the parcel misfortune is absolutely because of normal connection blunders, or is a consolidated impact of connection mistake and selfish node. In our project we have proposed an efficient method for detecting a selfish node which takes into account the various factors like the battery capacity of a node, power consumption in transmitting packets and to overcome the presence of selfish nodes. In this framework consists of degree of intrinsic selfishness (DeIS) and the degree of extrinsic selfishness (DeES). Under the distributed node-selfishness management, a path selection criterion is designed to select the most reliable and shortest path in terms of RNs'. The theoretical analysis and results show that the proposed model has better probability and efficiency.

Keywords— MANETs, Selfish Node, Node Misbehavior, Detection.

I. INTRODUCTION

MANETS are utilized as a part of numerous settings, for example, in mobile interpersonal organizations, crisis arrangement, keen transportation frameworks and so forth. Nodes in a MANET unreservedly move around while speaking with each other. These networks may perform within the sight of nodes with a selfish conduct, especially when working under vitality requirements. In the transmission of the parcels these selfish nodes will normally not collaborate, truly influence the network execution. Selfish nodes are the nodes partaking in the network, which are dithered to forward the parcels keeping in mind the end goal to spare the assets under the vitality requirements. Nodes which all are less regular may likewise neglect to coordinate either deliberately (a malignant conduct) or because of defective programming or equipment.

Node misconduct implies deviation from the first steering and sending. The source node can transfer parcels to the goal node through different nodes in MANET. The selfish nodes don't take an interest in the directing procedure, which purposefully postponement and drop the parcel. These misbehaviors of the selfish nodes will affect the productivity, dependability, and the decency. A selfish node does not play out the procedure identified by parcel sending function for information bundles irrelevant to it. The selfish node uses its restricted assets just for its own motivation as a result of the vitality and capacity limitations for every node in the MANET. It means to spare its assets to the greatest, so this kind of making trouble node disposes of every approaching bundle aside from those which are bound to it. The selfish nodes disregard to share their assets, for example, battery control, CPU time, and memory space to different nodes in MANET. This conduct is seen in the information connects/MAC layer, which is conclusive, particularly when the mobile nodes have little remaining force.

The main objective of the proposed work is to detect the selfish node in MANET using the audit based detection technique. The proposed method consists of a packet dropping detection scheme and a selfish node mitigation scheme. The selfish node is required to generate a trust report during each neighbor, which reports its previous communication reports to the neighboring node. Based on that report, the neighboring node detects if the selfish node has dropped packets. The neighboring node gathers the trust report to detect misreporting and then it finds out which node has dropped packets. A selfish node may report a false record to hide the dropping from being detected.

II. RELATED WORK

There are two primary methodologies to manage the selfish conduct in helpful networks. The main approach tries to spur the nodes to effectively partake in the sending exercises. For instance, in the creators displayed a strategy utilizing a virtual money called I.Chen et al. Proposed SPRITE, a credit-based framework for incentive support of selfish nodes in MANET correspondence. These incentivation strategies display a few issues, for example, the requirement for some sort of usage foundation to keep up the bookkeeping and they more often than not depend on the utilization or the like of carefully designed equipment. The COMMIT Protocol consolidates diversion theoretic systems to accomplish honesty and an incentivation installment plan to decrease the effect of selfish nodes on steering protocols. With respect to identification and prohibition approach, there are a few answers for MANETs and DTNs. A first learn about acting up nodes and how guard dogs can be utilized to identify them was presented in. The creators proposed an H.Jiang and W.Zhuang over the DSR protocol to recognize non-sending nodes, keeping up a rating for each node. Another plan for recognizing selfish nodes in view of setting mindful data was proposed. In past works, it has been demonstrated how some level of collaboration can enhance the discovery of selfish or getting out of hand nodes. The Confident protocol was proposed in, which consolidates a guard dog, notoriety frameworks, Bayesian channels and data acquired from a node and its neighbors to safely distinguish making trouble nodes. The framework's reaction is to segregate those nodes from the network, rebuffing then inconclusively.

All the more as of late, manuscripts have concentrated on DTNs. In the creator presents a model for DTN information transferring plans under the effect of node selfishness. A comparative approach is exhibited that demonstrates the impact of socially selfish conduct. Social selfishness are an expansion of traditional selfishness (likewise called singular selfishness). A social, selfish node can collaborate with different nodes of a similar gathering, and it doesn't participate with different nodes outside the gathering. In any case, these methodologies don't assess the impact of false positives, false negatives and vindictive nodes. For instance, the approach in just transmits positive identifications. The issue, as appeared in the assessment areas, is that if a false positive is created it can spread this wrong data rapidly on the network, detaching nodes that are not selfish. Subsequently, an approach that incorporates the dispersion of negative location two ends up noticeably essentially. Another issue is the effect of intriguing or vindictive nodes. Despite the fact that a notoriety framework, as the one exhibited in, can be valuable to moderate the impact of malignant nodes, it obviously relies on upon how are consolidated nearby and worldwide appraisals, as appeared in this manuscript. Another usage issue is the high forced overhead because of the flooding procedure keeping in mind the end goal to accomplish a quick dispersion of the data. Since our approach depends on gets in touch with, it has been demonstrated that the overhead is incredibly diminished.

III. Problem Definition

The primary issue in reproduction, distribution is the selfishness of nodes. That selfish node did not share its own particular memory to help different nodes. In any case, it appreciates all assets of different nodes, and limitedly shares its own particular assets to others. Such selfish conduct of node causes a difficult issue in network in the transmission of bundles. Those selfish nodes did not expend their own particular administrations like battery and memory stockpiling to transmit the information to others. At that point the whole network goes to retransmission arrange, at any rate this is troublesome. So that identifying specific selfish node is simple and apportioned copy of those nodes.

IV. Proposed Approach

Wherever, in the existing schemes, there is still having a problem of selfish nodes, which creates problem in accessing data and slow down the network performance. And also they are considering partial selfish nodes as selfish nodes, which may not create a problem sometimes so there may be a problem and also there is no server or control to monitor the replica allocation of nodes. The main objective of the proposed method is to monitor the selfish node properly in wireless networks. Here two types of method are implementing i.e., static and dynamic to find the selfish node. The selfish node is required to send a trusted information to the destination node. Based on that, the server monitors the selfish node at all the time. That means few data will send from source to destination for monitoring purpose. If the relay node is properly to send all the data to destination at any time data transfer will not stop that node is called non-selfish
node.

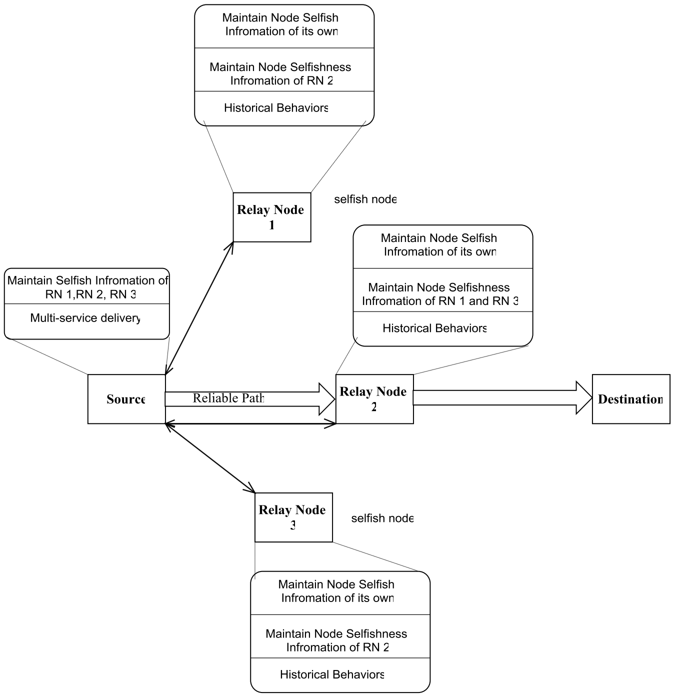

Maintain Node Selfish Infromation of its own
Maintain Node Selfishness Infromation of RN 2
Historical Behaviors
Relay Node 1
selfish node
Maintain Node Selfish Infromation of its own
Maintain Node Selfishness Infromation of RN 1 and RN 3
Historical Behaviors
Maintain Selfish Infromation of RN 1,RN 2, RN 3
Multi-service delivery
Source
Reliable Path
Relay Node 2
Destination
Relay Node 3
selfish node
Maintain Node Selfish Infromation of its own
Maintain Node Selfishness Infromation of RN 2
Historical Behaviors

Fig.1. Proposed Architecture

E2E Algorithm:

- Step 1: Every source selects the most reliable and shortest path and provides the optimal incentives to the RNs within the selected path for the multi-service delivery.

- Step 2: For delivering multi-services, the sources find some paths by virtue of the traditional routing protocol.

- Step 3: Nevertheless, these paths may not be all reliable for successfully forwarding, multi-services due to the node-selfishness of the RNs within these paths.

- Step 4: The RN's DeIS SI is defined as the degree reflecting the effects of intrinsic factors on its selfish behavior, while the RN's DeES SE is defined as the degree reflecting the effects of extrinsic factors on its selfish behavior.

V. Results And Analysis

Amid the re-enactment, every node begins its exclusive from an irregular spot to an arbitrary picked goal. Once the goal is achieved, the node takes a rest timeframe in second and another irregular goal is picked after that delay time. This procedure rehashes all through the recreation, creating constant changes in the topology of the hidden network. E2E is the proportion of the quantity of information parcels gotten by the goal node to the quantity of information bundles sent by the source mobile node. It can be assessed regarding rate (%).

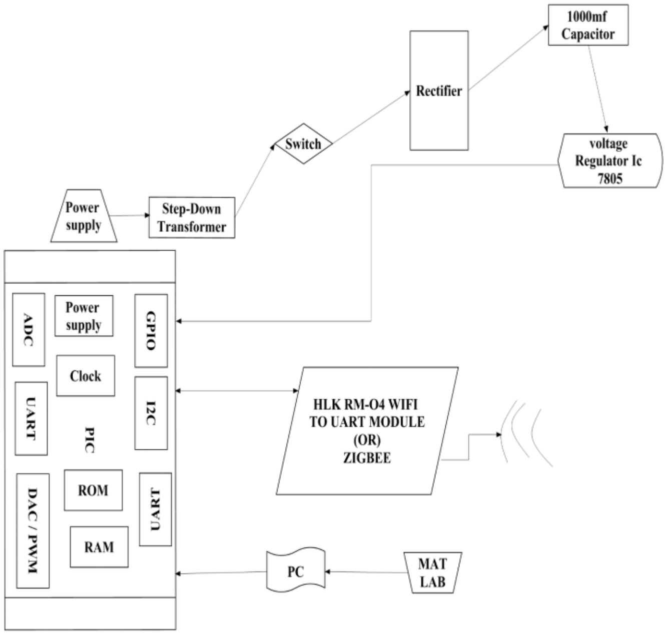


Fig.2Server

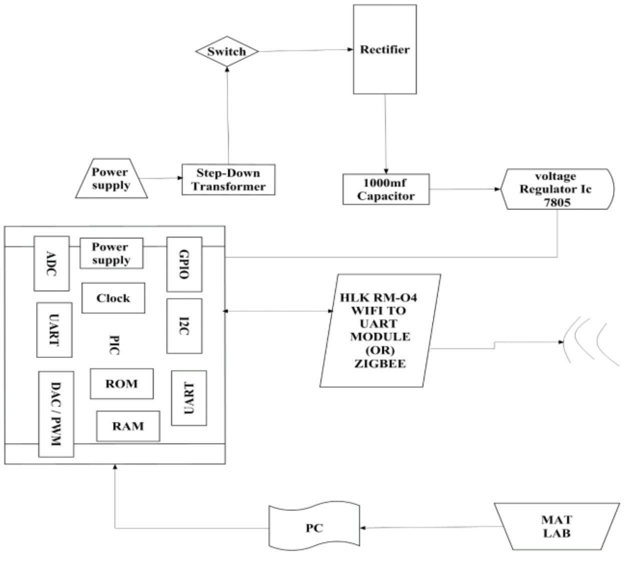


Fig.3 Client 1

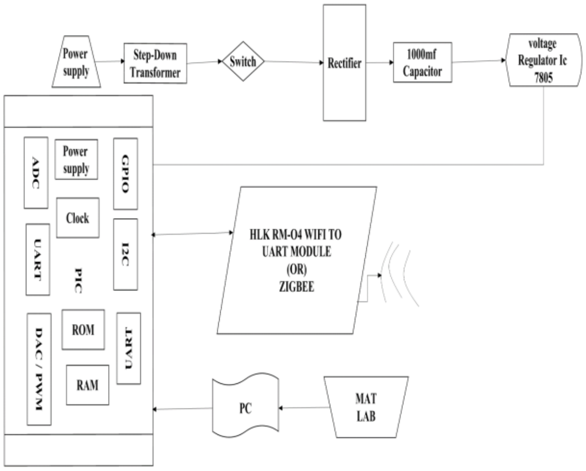
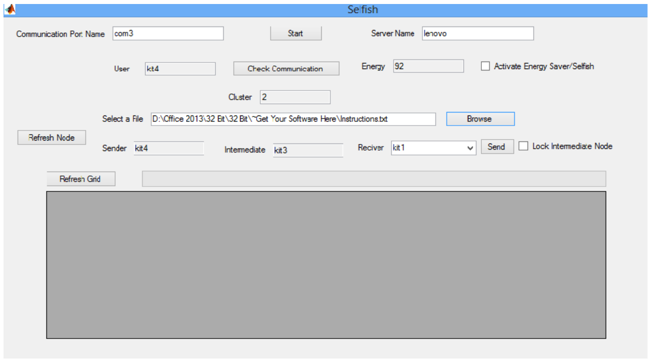


Fig.4 Client 2

Simulation Result



Communication Por. Name com3

Server Name lenovo

User kt4

Energy 92

□ Activate Energy Saver/Selfish

Cluster 2

Select a File D:\Office 2013\32 Bit\32 Bit\~Get Your Software Here\Instructions.txt

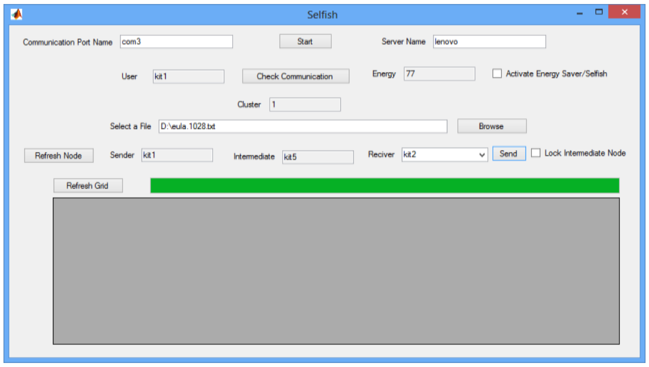
Sender kit4

Intermediate kit3

Reciver kit1

□ Lock Intermediate Node

Fig.5. Main form



Communication Port Name: com3

Server Name: lenovo

User: kit1

Energy: 77

□ Activate Energy Saver/Selfish

Cluster: 1

Select a File: D:\eula.1028.txt

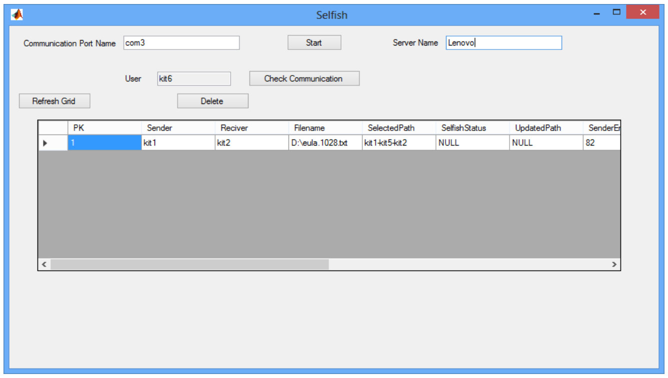
Sender: kit1

Intermediate: kit5

Reciver: kit2

□ Lock Intermediate Node

Fig.6. File Send to Receiver Using Intermediate Node



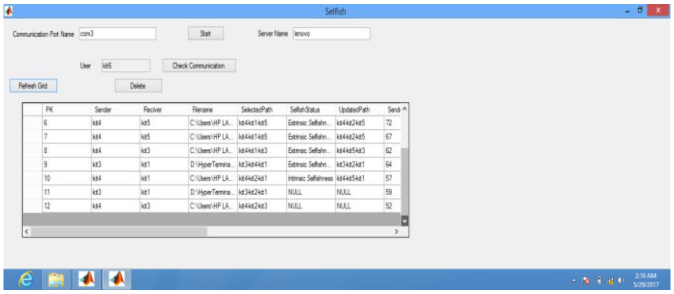
Communication Port Name: com3

Server Name: Lenovo

User: kit6

	PK	Sender	Reciver	Filename	SelectedPath	SelfishStatus	UpdatedPath	SenderEı
▸	1	kit1	kit2	D:\eula.1028.txt	kit1-kit5-kit2	NULL	NULL	82

Fig.7. View Receiveing File



Communication Port Name: com3

Server Name: lenovo

User: kit6

	PK	Sender	Reciver	Filename	SelectedPath	SelfishStatus	UpdatedPath	Send
	6	kit4	kit5	C:\Users\HP LA...	kit4-kit1-kit5	Extrinsic Selfishn...	kit4-kit2-kit5	72
	7	kit4	kit5	C:\Users\HP LA...	kit4-kit1-kit5	Extrinsic Selfishn...	kit4-kit2-kit5	67
	8	kit4	kit3	C:\Users\HP LA...	kit4-kit1-kit3	Extrinsic Selfishn...	kit4-kit5-kit3	62
	9	kit3	kit1	D:\HyperTermina...	kit3-kit4-kit1	Extrinsic Selfishn...	kit3-kit2-kit1	64
	10	kit4	kit1	C:\Users\HP LA...	kit4-kit2-kit1	Intrinsic Selfishness	kit4-kit5-kit1	57
	11	kit3	kit1	D:\HyperTermina...	kit3-kit2-kit1	NULL	NULL	59
	12	kit4	kit3	C:\Users\HP LA...	kit4-kit2-kit3	NULL	NULL	52

Fig.8. Server Form

VI. Conclusion

The Proposed system introduced the distributed framework of the node-selfishness management, where every RN manages its Node Selfishness Information that is Intrinsic and Extrinsic information and other nodes NSI and every source node manages the RNs' NSI in distributed SeWNs. In this framework, the RN's models of intrinsic and extrinsic selfishness have been developed to manage its DeIS and DeES, and the other RNs' NSI has been obtained in terms of the RNs' historical behaviors and their recommended NSI. Under this distributed framework of the node-selfishness management, the path selection criterion has been designed to select the most reliable and shortest path for the multi-service delivery.

VII. Future Work

In the future, we are going in to the development of the proposed system. In the future aim is mainly an effort to implement secret key mechanism other kind of wireless network for providing better service and security. So the use of this mechanism achieves highest delivery rate of packet from source to destination. Moreover the future system includes the use of cluster based, selfish node identification through this, we can reduce the detection time of selfish node along with increased throughput.

References

[1] B. Swetha, D.B. Rao, P.N. Rao, "*Intelligent Anti-Theft Finding Scheme Towards Itrust Establishment in Delay Tolerant Networks Using VANET*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.9, pp.50-56, 2014.

[2] J.Li, Q.Yang, and K.S.Kwak, *"Neural-network based optimal dynamic control of delivering packets in selfish wireless networks,"* IEEE Commun. Lett. vol.19, no.12, pp.2246–2249, Dec.2015.

[3] H.Jiang and W.Zhuang, *"Cross-layer resource allocation for integrated voice/data traffic in wireless cellular networks,"* IEEE Trans. Wireless Commun., vol.5, no.2, pp.457–468, Feb.2006.

[4] F.Bao, I.Chen, M.Chang, and J.Cho, *"Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,"* IEEE Trans. Netw. Serv. Manage., vol.9, no.2, pp.169–183, Jun.2012.

[5] Shanmugapriya R. "*Parallel Networks For Enhancing And Efficient Delay Bounds Based Trust Management*", International Journal of Applied Engineering and Technical Research-IJAETR. Vol.1, Issue.1,pp.1-9, 2017.

[6] S. Jain, "*Black Hole Attack in Delay Tolerant Networks: A Survey*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.4, pp.172-175, 2014.

[7] H. Zhu, X. Lin, and R. Lu, *"SMART: A secure multilayer credit based incentive scheme for delay-tolerant networks,"* IEEE Trans. Veh. Technol., vol.58, no.8, pp.4628–4639, Oct.2009.

[8] P.Kyasanur and N.F.Vaidya, *"Selfish MAC layer misbehavior in wireless networks,"* IEEE Trans. Mobile Comput., vol.4, no.5, pp.502–516, Sep.2005.

[9] Z.Ji and K.J.R.Liu, *"Multi-stage pricing game for collusion-resistant dynamic spectrum allocation"* IEEE J.Sel.Areas Commun., vol.26, no.1, pp.182–191, Jan.2008.

[10] Y.Rebahi, V.E.Mujica-V, and D.Sisalem, *"A reputation-based trust mechanism for ad hoc networks,"* in Proc. IEEE Symp. Comput. Commun. Jun.2005, pp.37–42.

[11] C.E.Perkins, E.M.Royer, S.R.Das, and M.K.Marina, *"Performance comparison of two on-demand routing protocols for ad hoc networks,"* IEEE Pers. Commun., vol.8, no.1, pp.16–28, Feb.2001.

[12] Y.Xiao and H.Li, *"Voice and video transmissions with global data parameter control for the IEEE 802.11e enhance distributed channel access"*, in IEEE, vol.15, issue.11, pp.1041–1053, Nov.2004.

[13] M.v.d. Schaar, Y.Andreopoulos, and Z.Hu, *"Optimized scalable video steaming over IEEE 802.11a/e HCCA wireless networks under delay constraints"*, in IEEE, vol.5, issue.6, pp.755–768, Jun 2006.

[14] R.Dai, P.Wang, and I.F.Akyildiz, *"Correlation-aware QoS routing with differential coding for wireless video sensor networks"*, in IEEE, vol.14, issue.5, pp.1469–1479, Oct.2012.