

DETECTION OF SELFISH NODE IN WIRELESS NETWORK

Ms.R.Hema Priya¹, Mr.P.Bright Prabaha²

¹P.G.Student, ²Assistant professor, M.tech

Dept of Electronics and communication Engineering

Parisutham Institute of Technology & Science, Thanjavur, Tamil Nadu, India

Abstract: In Wireless Network communication, every node transmits data packets to further nodes. In ideal situation all the nodes forward packets to other nodes according to their requirements. Presence of selfish nodes is a very big problem in Wireless Networks. A selfish node doesn't forward packets and utilize to its own profit but it is hesitating using personal resources for others. If such activities occur within most of the nodes in the network, the network is interrupted. Selfish behavior detection is an essential condition in wireless networks. In this project we have described an efficient method for detection and punishment of a selfish node. Under the distributed node-selfishness management, a path selection criterion is designed to select the most reliable and shortest path in terms of RNs'. Degree of intrinsic selfishness nodes affected by their available resources, and the optimal reasons are determined by the source to stimulate forwarding multiservice of the RNs in the selected path.

Index term: RN s, multi services, shortest path, intrinsic selfishness, extrinsic selfishness

I. INTRODUCTION

Maintaining connectivity within a wireless network is the precondition for guaranteeing efficient networking relying on the functions of routing, power control, topology control, etc. Given the increase of smart devices in intelligent networks, each node is expected to be endowed with smart autonomic functions. By nature, the individual network nodes would prefer to act selfishly rather than altruistically in distributed network situations[2]. For instance, while forwarding the packets of other nodes at the cost of sacrificing their own limited resources, they expect to satisfy some of their own objectives, such as maximizing their own transmission rate and/or minimizing their own resource consumption. To enforce cooperation among nodes and detect selfish nodes in ad hoc wireless networks, various collaboration schemes have been proposed in the literature. Majority of these proposals are based on trust and reputation frameworks which attempts to identify misbehaving nodes by suitable decision making systems and then isolate or punish them. The reputation of participating nodes is built based on local observation at the node, second-hand observation at other nodes or both. To address the issue of selfish nodes in a WMN, this paper presents a scheme that uses local observations in the nodes for detecting node misbehavior[1]. The scheme is applicable for on-demand routing protocol like AODV, and uses statistical theory of inference and clustering techniques to make a robust and reliable classification (cooperative or selfish) of the nodes based on their packet

forwarding activities as observed by their neighbors. In addition, it introduces some additional fields in the packet header for AODV protocol so that detection accuracy is increased.

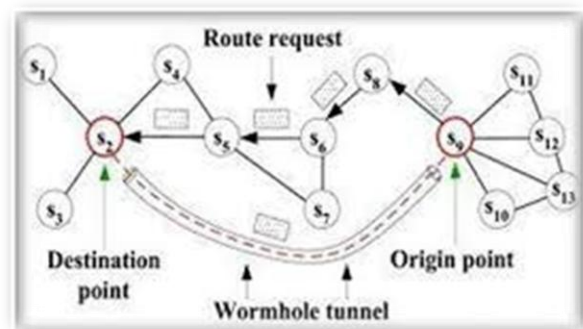


Fig 1. Node Formation

A .Brief Review of Network Security

This section shows security requirements, possible attacks in traditional networks. Passive attack happened without the interrupting in the communication operations. For the Active attack node works as active node. It can perform the operations like interruption, modification, or fabrication, at the time of attack directly. In the Internal Attack nodes are the part of network in order to perform attack. Whereas External Attack nodes does not belong the network in order to perform attack. In the purpose of Black hole Attack, malicious user broadcast the message having the false information of shortest path. This shortest path is work for the attack. Some time it also makes the set of intermediate nodes and works as an attacker. The operation can perform like routing loops and forwarding packets dropping packets. It will degrade the quality of services. In such cases, selfishness is determined based on a predefined threshold value of a single set of actions such as number of dropped packet and packet forwarding rate of a particular relay node for a requestor. E.g., the packet forwarding rate can be defined as follows:

$$\text{Forwarding rate} = \frac{\text{number of packets forwarded}}{\text{number of packets received}}$$

based on the total number of packets a node has successfully forwarded in comparison to the number of packets it has received. The Routing protocols are responsible to perform dynamic routing and information sharing as well. Table Driven Protocol is the type approach the protocol will store the table in order to get the route of destination. With the help of that table the route will decides and forward the packet to the destination node [4]. There are many table driven protocol has developed like DSDV, WRP etc. this approach is also known as the proactive protocols. On

Demand Protocol is another approach to route the packet in the wireless network. This approach does not have any pre decided route. Authentication is needed in order to be sure about the identity of the sender or receiver of a message. The attack is called masquerading, that is pretending to be somebody else. Since in mobile ad hoc networks there are no central authorities available for certificates and key distribution to authenticate identities, it becomes harder to detect corrupted nodes. A distributed kind of authentication is needed. All other services depend on authentication. Confidentiality concerns the content of a message. Only the sender and the receiver are supposed to know the content. Attacks include message interception (man in-the-middle attacks), content release to other parties, etc. In mobile ad hoc networks, wireless link broadcast facilitates eavesdropping and key distribution is more difficult. Integrity ensures that system assets and transmitted information are modified only by authorized parties. Modification includes writing, changing, changing status, deleting, creating, and the delaying or replaying of transmitted messages. Availability of services or devices is attacked by denial of service.[8] This is traditionally done by interruption, network or server overload. With mobile ad hoc networks of potentially low powered devices, sleep deprivation (engaging the devices CPU until the battery power is exhausted) or incorrect forwarding of messages are effective attacks. Network overload is easier on small bandwidth wireless links and bogus routing advertisements are harder to detect in a dynamic environment. Access Control restricts resources, services or data to special identities according to their access rights or group memberships for instance. Access control enforces authorization. Means to attack are again masquerading, message interception and modification, forging, etc. Since with mobile ad hoc networks there is no infrastructure and the network is potentially highly dynamic, it is hard to detect corrupted nodes. In order to exercise access control, distributed authentication management is needed. Non-Repudiation is about not being able to deny having sent or received a message. A typical attack is masquerading. Threats endanger the security, they can be deliberate or accidental. Attacks are materialized threats. Safeguards aim at protecting against threats and can be physical control, mechanism, policy, procedure to protect assets from threats. A policy governs whether a service is used. Vulnerability is the absence of a safeguard. Mechanisms provide services. Attacks are interruption for availability, interception for confidentiality, modification for integrity, fabrication for authenticity. Attacks are passive (release of contents, traffic analysis) or active (masquerade, replay, modification, denial of service).

B. Networks Special Properties

Mobile ad hoc networks exhibit properties different from fixed networks or infrastructure based wireless networks. These properties make it harder to implement security services or even exhibit vulnerabilities to different and additional security attacks: Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. Constraints in bandwidth are caused

by the limits of the air interface with fading and noise. Computing power in mobile devices require security mechanisms to be low in computation overhead. Battery power in mobile devices can lead to application specific trade-offs between security and longevity of the device. Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes since routes in this environment change frequently. It is difficult to employ mechanisms like firewalls, because the border between being inside or outside the network is blurred. Self-organization is a key property of ad hoc networks. They cannot rely on central authorities and infrastructures. Therefore, trust management has to be distributed and adaptive. On the bright side, self-organization leads to inherent better fault tolerance thanks to the absence of the potential bottleneck of centralized authorities. Latency is increased by the fact that in order to save battery power devices can decide to sleep and only wake up, when there is a message for them, which increases the reaction time of the device by the time it takes to wake up. Inherently the round-trip-time for packets is increased in wireless multi-hop networks; rendering message exchange for security more expensive. Multiple paths are likely to be available given sufficient node density. [6]This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding. This means that multiple copies of a packet or parts of it can be sent over different paths to increase the probability of a packet actually arriving at a destination unchanged. A wireless network which consists of nodes exhibiting a selfish behavior is hence referred to as a selfish wireless network (SeWN). In such network situations, the selfish behavior network nodes may reduce the throughput of the nodes and/or their integrity, thus potentially leading to degraded network connectivity. The node-selfishness of the network node is affected by some intrinsic and extrinsic factors, such as its own energy and bandwidth resources, the QoS requirements and the employed incentive mechanisms. For improving the network performance, the node individuals need to obtain the information on the node-selfishness of the other nodes and to determine the relationship between the aforementioned factors and the node-selfishness. In such distributed network scenarios, each network node may obtain the aforementioned information, directly collected by it and/or indirectly received from its neighboring nodes. Accordingly, each network node should establish a distributed node-selfishness management for managing therefore mentioned information on the node-selfishness, whilst improving the network performance of delivering multiservice, i.e., the reliability of the selected path and the successful probability of delivering multi-services. A node desires to recognize if another node is believable, in the intelligence that a replica can be paid back, or served upon request to divide a memory space in a MANET. By way of the considered degree of selfishness, a novel tree that symbolizes relationships among nodes in a MANET is proposed for replica allocation termed The key strength of the SCF-tree-based replica allocation selfish nodes.

II. WORKING PRINCIPLE

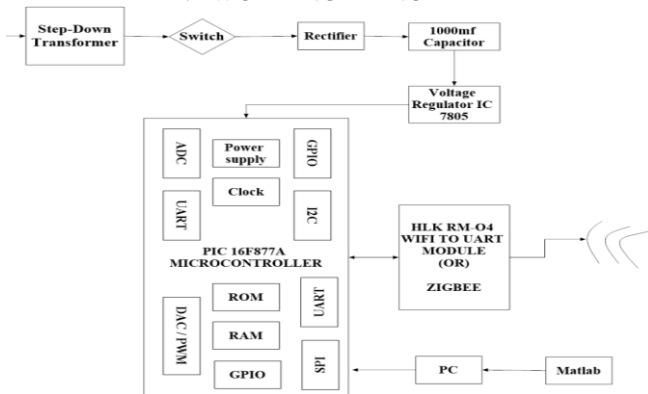


Fig.2. Block Diagram

C. Selfish Alert Algorithm

Algorithm for detection of selfish nodes in a wireless networks. It uses reliable clustering of the nodes. The algorithm has a high detection rate. The proposed algorithm initially clusters the neighbors of a monitoring node and then classifies the clusters into selfish node. This proposed algorithm initially plots the neighbors of a monitoring node into clusters and then classifies the clusters into selfish and cooperative. [8] Detecting selfish nodes that drops packets based on the level of reputation. This mechanism decides a node as selfish when the number of packets forwarded by a mobile node to its neighbor is equal to the number of packets received by that node from its neighbors. The proposed algorithm initially maps the neighbors of a monitoring node .

III. III PROPOSED SYSTEM

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 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 is implement i.e., static and dynamic to find the selfish node. The selfish node is required to send trust 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.

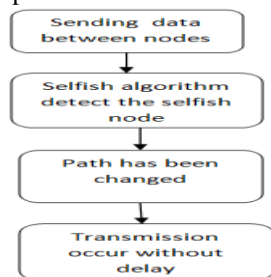


Fig.3 . Flow diagram

Advantages

- It reduces the loss of pack by selecting optimal shortest path for multiservice delivery.
- The source should reduce the selection frequency and maintain the reliability of the selected path.

IV. SIMULATION AND OUTPUT

The proposed protocol is evaluated with network simulator ns-2 (version 2.29) [5] with parameters presented in Table III. The objective is to evaluate the efficiency of the algorithm and compare its performance with the protocol proposed by Wang et al in [3]. At the start of the simulation, a fraction of nodes are chosen randomly as the selfish nodes. A selfish node adopts either of the two strategies--dropping RREQs (DROP_REQ) or dropping RREPs (DROP_REP). In both cases, control packets are dropped with a constant probability. For DROP_REP, a selfish node always rebroadcasts RREQs even if it has a route in its cache. To evaluate the detection efficiency and speed, the packet dropping probability is varied from 1.0 to 0.1. β is chosen as 0.4 to have the best tradeoff between detection rate and false positive rate.

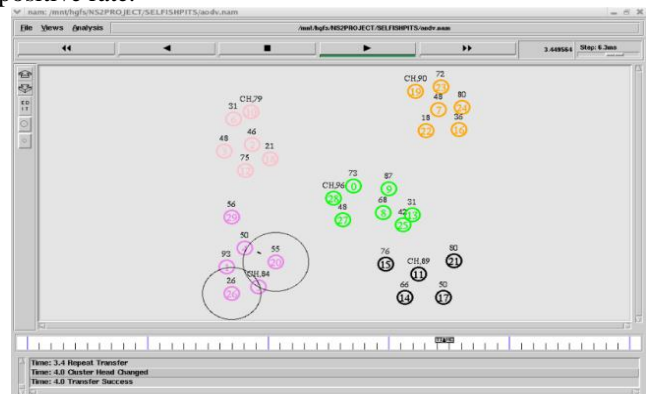


Fig -4 ns-2 simulation output

It is thus essential for intermediate nodes to assist in disseminating the RREQ until the path to the intended destination is found and an RREP unicast back to the source node to establish a bidirectional routing flow prior to actual data transmission. This process can only be successfully accomplished if all nodes cooperate and participate in the forwarding of these control messages.

B. Selfishness in AODV

Several scenarios of selfishness occurring in AODV include:

- Nodes do not forward the received RREQ messages to their corresponding next hops, the established route does not pass through these nodes;
- Nodes do not generate RREP messages in response to RREQs for destinations that they have routes to, or do not assist in unicasting RREPs back to source to complete the route setup process;
- Nodes do not advertise Route Error (RRER) messages when link error is detected or whenever necessary, causing other nodes to be unaware of the current faulty state, thus wasting energy transmitting packets that could not reach their intended destinations;
- Nodes assist in route setup but do not transmit data packets because they are only interested to use the

established route for their own transmission, thus data packets from other nodes do not reach their destinations. The aforementioned examples of selfish behaviour can arise in real networks and require effective measures to mitigate the adverse effects.

V. CONCLUSION

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. [10] Additionally, the optimal incentives have been adjusted by the source for maintaining the path reliability of the E2E multi-service delivery. We have designed selfish node monitoring system based on communication by using NS2 simulation software to provide live monitoring and detect selfish node. When detects selfish node then the node is automatically change to transfer the data to destination.[9] In future, the system will implement the real time monitoring through dynamic mode of the find selfish node. Also change over the node automatically to transfer the data. WIFI or ZIGBEE wireless device is used to transfer the data from source node to destination node.

REFERENCES

- [7] P. Kyasanur and N. F. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE Trans. Mobile Computer.*, vol. 4, no. 5, pp. 502–516, Sep. 2005.
- [8] Z. Ji and K. J. R. Liu, "Multi-stage pricing game for collusion-resistant dynamic spectrum allocation," *IEEE J. Sel. Areas Communication.*, vol. 26, no. 1, pp. 182–191, Jan. 2008.
- [9] Y. Rebahi, V. E. Mujica-V, and D. Sisalem, "A reputation-based trust mechanism for ad hoc networks," in *Proc. IEEE Symp. Computer. Communication.*, Jun. 2005, pp. 37–42.
- [10] 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. Communication.*, vol. 8, no. 1, pp. 16–28, Feb. 2001.

- [1] J. Li, Q. Yang, K. S. Kwak, and L. Hanzo, "The connectivity of selfish wireless networks," *IEEE Access*, vol. 3, pp. 2814–2827, Nov. 2015.
- [2] J. Li, Q. Yang, and K. S. Kwak, "Neural-network based optimal dynamic control of delivering packets in selfish wireless networks," *IEEE Communication. 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 communication.*, 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. Network. erv. Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.
- [5] I. Chen, F. Bao, M. Chang, and J. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel Distribution. Syst.*, vol. 25, no. 5, pp. 1200–1210, May 2014.
- [6] 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.