REVIEW OF DETECTING SELFISH NODES & ESTABLISHING SECURE ROUTE IN MANET

Nitesh Kumar[#1], Dr. Sandeep Dubey[*2]

[#1] Scholar Student,, [#2]Asst. prof.& CSE Department & RKDF University
Bhopal,(M.P.), India

Abstract

MANET consists of a collection of MOBILE nodes that is it have infrastructure less network and without any centralized node is wireless network. Each node is itself sender, receiver and router, as well as each node are allowed to move freely in the MANET hence making routing difficult. Thus the main activity in the MANET is to search for suitable secure routes in the middle of the message delivery in an efficient manner. But there are various security issues in the network such as packet dropping; ideally, there is no non-cooperative guarantee in the network between the nodes. Such a behaving node is called a selfish node. The presence of selfish nodes in the MANET causes damage to the entire communication system.

Keywords: MANET, Selfish nodes, watchdog techniques, Hash based technique, AODV.

1. Introduction

MANET is a combination of more than one wireless node and has the limitation of bringing together the information coming together without any kind of help. Each gadget goes into the ad-hoc network as a switch and end framework. The network topology in wireless MANET is dynamic because of the mix of nodes changing over time, looking at the portability of nodes, sections of new nodes, and the battle of nodes. Thus, beneficial steering protocols are necessary to communicate these nodes.

Abnormal and snappy topological changes, wireless network dynamic nature, portability of nodes and confined battery power raise various troublesome in construction up a directing protocol. On account of colossal difficulties in arranging directing protocol for MANET, different advancements as of late concentrating on giving perfect answer for steering. Along these lines, a perfect directing protocol that can cover most of the client prerequisites or applications and also adjust up to the severe lead of the wireless medium is continually appealing.

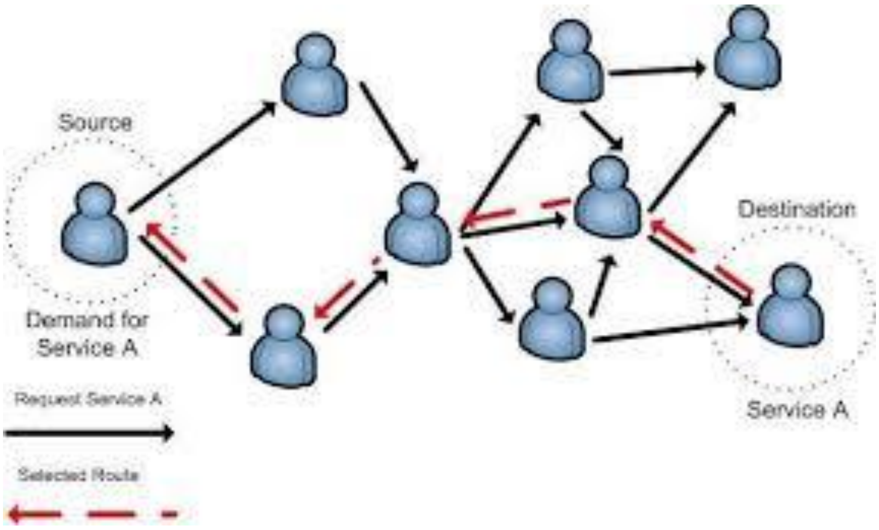

Figure 1:- Routing Protocol in establish path in MANET's

Impromptu nodes are gadgets that have the ability to recognize the presence of other such gadgets to allow information sharing and correspondence. In addition, it should also have the ability to recognize the associated characteristics and types of administrations. The measurement of wireless nodes will change due to the portability of the nodes, the steering information also changes to follow the change in connection availability. As a result, the topology of the network is an unreliable arrangement that is dynamic and modifications are now randomized each time, which appear differently with respect to the actual type of systemic wired network.

2. Related Work

Enrique Hernandez-Orallo et al 2012, MOBILE Ad-hoc network s (MANETs) are made out of MOBILE nodes associated by wireless joins without utilizing any prior framework. MANET nodes depend on network participation plans to appropriately work, sending traffic inconsequential to its own utilization. Be that as it may, in reality, most nodes may have a selfish conduct, being reluctant to advance packet for others so as to spare assets. In this way, detecting these nodes is fundamental for network execution. Guard dogs are utilized to distinguish selfish nodes in PC network s. An approach to diminish the discovery time and to improve the exactness of guard dogs is the communitarian approach. This paper proposes a communitarian guard dog dependent on contact spread of the identified selfish nodes. At that point, we acquaint a scientific model with assess the discovery time and the expense of this communitarian approach. Numerical outcomes show that our community-oriented guard dog can significantly diminish the general recognition time with a decreased overhead.

Sunil Kumar et al 2016, Due to the restricted transmission capacity of MOBILE nodes in MOBILE Ad-hoc network s (MANETs), the middle of the road nodes are utilized in multi-bounce style for sending the packet for different nodes. In any case, the multi-bounce correspondence causes a significant issue that a node may go about as selfish by avoiding sending the packet for different nodes so as to spare its energy and registering assets. A selfish node endeavors to use the network assets for its own advantages, yet hesitant to spend its assets for other people. In this manner, it is extremely critical to examine and segregate the selfish nodes from the network so as to trim down the dangers from such nodes, and improve the security of the network. This paper presents a near investigation of most conspicuous selfish node recognition and alleviation strategies proposed by the researchers in the literature.

Lien-Wen Wu et al 2010, MOBILE Ad-hoc network s (MANET) are made out of numerous MOBILE gadgets with wireless interfaces. The network s work well with no framework. The source node can transfer packet to the destination node through different nodes in MANET. In any case, the mischievous activities of nodes are regular wonder in MANET. These mischievous activities of the selfish nodes will affect the proficiency, the dependability, and the decency in MANET. In this paper, we propose an edge based strategy to build the selfish nodes discovery rate and lessening the bogus identification rate. At long last we will utilize the ns-2 test system to watch the location rate and the bogus recognition rate at various moving pace of the nodes.

H.Cai and D.Y. Eun Power law inter meeting time in MOBILE Ad-hoc network s [5] In this paper it portrays the key measurements in MANETs and they use end to defer sending algorithm. This protocol will examine about the connection between the size of the limit and time size of intrigue, and their impact on the entomb meeting time, that just evacuating the limit it can rapidly change the bury meeting time dissemination from exponential to control law by considering a basic irregular stroll in an open space. This outcome shows the exhibition examination, and protocol structure so as to endure the force law dissemination of the intermeeting time in MANET.

3. Problem Statement

The imminent destructive impact of selfish nodes in the MANET is a significant issue. Because selfish nodes do not participate in the routing process of the overall network which leads to degradation of network performance. Also, selfish nodes deliberately drop packets and delay messages. These abuses of selfish nodes affect efficiency, objectivity, and reliability. Hence, these nodes have to be detected and ignored, ensuring a safe route and establishing communication in the MANET.

Side effects of identifying the selfish behavior of nodes are as follows:

- Non-participation in routing
- No broadcasts or replies to Hi messages
- Intentional postponement of route request (RREQ) packet
- Data packet drop
- Selfish Behaviour Depending on the Nodes Energy

4. Proposed Methodology

4.1.Proposed work

The proposed work uses an algorithm based on cryptographic hash-based AODV(HAODV) to identify node misbehavior. HAODV is a technique by which a message is authenticated by identifying a selfish node and establishing a secure route that will prove that the message is successfully reaching the source from the destination. The HAODV algorithm has the following steps: initialization stage, hash generation at source, hash generation at the destination, detection selfish node, establishing a secure route and packet forwarding phase.

4.2.Objective

- The objective of this research is to develop HAODV efficiently algorithm to reduce the false detection rate (FDT) and increase the true detection rate (TDR) of selfish nodes in MANET.
- To detect selfish nodes through hash technique and establish a secure route in MANET via AODV
- Reducing selfish nodes increases the network 's energy efficiency and improve MANET performance.
- This research is to analyze and verify the performance using NS 2.31.

4.3.Flow diagram of proposed methodology Description

The research is an AODV encryption algorithm utilized so as to guarantee the trustworthiness of the detected data conveyed by the nodes to the next following after nodes. The malicious behaviour may occur in the middle of the nodes on transmission of the identified information thus so as to invalidate that conditions we use AODV encryption algorithm to guarantee the honesty between the nodes and to keep away from false impersonated nodes in the network. So that the selfish nodes may not get advantage from the undertaken nodes in the network and transmission is done clearly.

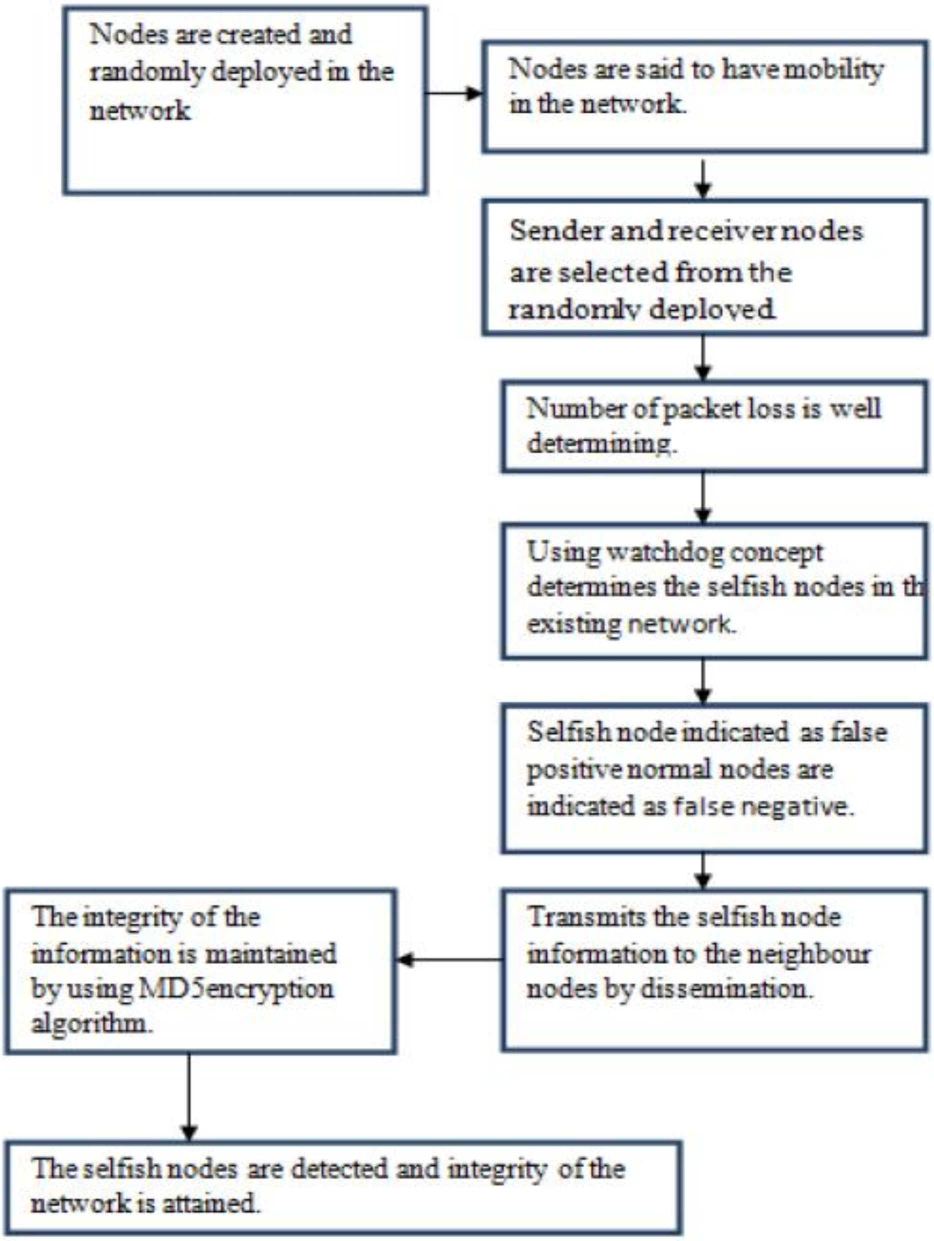
Nodes are created and randomly deployed in the network
Nodes are said to have mobility in the network.
Sender and receiver nodes are selected from the randomly deployed
Number of packet loss is well determining.
Using watchdog concept determines the selfish nodes in th existing network.
Selfish node indicated as false positive normal nodes are indicated as false negative.
Transmits the selfish node information to the neighbour nodes by dissemination.
The integrity of the information is maintained by using MD5encryption algorithm.
The selfish nodes are detected and integrity of the network is attained.

Figure 2: Flow diagram of proposed methodology Description

5. Conclusion

We proposed a hash based AODV technique for detecting Selfish nodes. Selfish nodes in the network don't offer any types of assistance to other and reserve resources to itself. Here we proposed a method for detecting Selfish nodes, which don't send Route Request(RREQ) packet and checked with ns2.31 simulator system, we analyzed the false detection rate, detection rate with various moving rates, distinctive number of Selfish nodes in the network and with various activity holdoff times, we watched high detection rate when the number of Selfish nodes are less and low activity holdoff time where as false detection rate is less when the activity holdoff time is high.

Reference

[1].Hernandez-Orallo Enrique ; Manuel D. Serrat ; Juan-Carlos Cano ; Carlos T. Calafate ; Pietro Manzoni, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog ", IEEE Communications Letters (Volume: 16 , Issue: 5 , May 2012), pp 642 – 645.

[2].Kumar Sunil , Dutta Kamlesh, and Sharma Girisha , "A detailed survey on selfish node detection techniques for mobile Ad-hoc Networks", Fourth International Conference on Parallel 2016, Distributed and Grid Computing (PDGC),

[3].Wu Lien-Wen and Yu Rui-Feng , "A threshold-based method for selfish nodes detection in MANET", International Computer Symposium (ICS-2010).

[4].Cai H. and Eun D.Y., "Crossing over the bounded domain: from Exponential to power-law intermeeting time in mobile Ad-hoc Networks", IEEE/ACM vol.17, no.5, oct.2009 pp.1578-1591.

[5].Sergio Marti, "Mitigating routing misbehaviour in mobile Ad-hoc net-works", Proceedings of ACM the 6th annual international conference on mobile computing and networking 2000.

[6].MolvaR., and Michiardi P., "Core: A collaborative reputation mechanism to enforce node cooperation in mobile Ad-hoc Networks." Institute Eurecom-Research Report RR-02-062 (2001).

[7].Orallo Hernandez, Enrique "Improving Selfish node detection in MANETs using a collaborative watchdog."I EEE Communications Letters, vol 16.5 (2012): pp 642-645.

[8]. Tarag Fahad, and Askwith Robert. "A Node Misbehaviour Detection Mech-anism for mobile Ad-hoc Networks." proceedings of the 7th Annual Post Graduate Symposium on The Convergence of Telecommunications on Networking and Broadcastin 2006