IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Defence Scheme against Selfish Node Attack in Manet

Khushbu[1*], R.K. Bathla[2]

[1]Department of phd scholar MadhavUuniversity Sirohi ,Rajasthan-307026, India
[2]Professor in Madhav University sirohi, Rajasthan-307026, India

Corresponding Author:khushbu.yadav91@yahoo.com

DOI: https://doi.org/10.26438/ijcse/v7i5.15471550 | Available online at: www.ijcseonline.org

Accepted: 14/May/2019, Published: 31/May/2019

Abstract- Mobile Ad hoc network (MANET) suffers from different security issues. Ideally, not all nodes in MANET cooperate in forwarding packets because of non-malicious intention. This node is called selfish node and it behaves so due to its internal state such as limited energy concerns. Selfish nodes drop packets and that harms the process of routes establishment and relaying packets. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name Mobile Ad hoc Networks or MANETs. They have many potential applications, especially in military and rescue operations such as connecting soldiers in the battle field or establishing a temporary network in place of one which collapsed after a disaster like an earthquake. In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes use routing protocols such as AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing). Mobile ad-hoc networks are usually susceptible to different security threats and selfish attack is one of these. In Selfish attack, a malicious node which absorbs and drops all data packets and routing packets makes use of the vulnerabilities of the on demand route discovery protocols, such as AODV

Keywords- IDS, MANET, Security, Selfish node attack, DSR (Dynamic Source Routing), AODV (Ad hoc On-Demand Distance Vector)

I. INTRODUCTION

Ad hoc networks are defined as networks that lack a fixed infrastructure and hence are flexible and adaptive in nature. Ad hoc networks consist of individual devices, also known as nodes that communicate with each other wirelessly without a central access point. The devices, hence, do not rely on a base station to coordinate the flow of messages.[1] Instead, the individual network nodes pass packets to each other within the network. Ad hoc networks can be used in multiple applications such as creation of communication networks at times of emergency when the existing communication is damaged due to natural disasters, creating conferencing networks for office use that do not rely on the internet, home networking and personal area networks, especially with Bluetooth devices associated with a single person. A mobile ad hoc network (MANET) is defined as an ad hoc network that uses mobile nodes that are arbitrarily located. The nodes in a MANET are highly dynamic and may join and leave the system frequently. Since the nodes are highly mobile, the topology of the network changes rapidly. Hubs are associated by different kinds of directing convention ideas. Essentially they are two sorts Reactive what's more, Proactive conventions. In Reactive, courses are resolved when way required to goal, it's an on-request steering convention (AODV, DSR, etc.,),where as in proactive convention, all hubs keep up tables portrayal , the whole topology of the system (OLSR, DSDV, etc.,). Typically directing conventions are associated each hub in the system and hubs carries on agreeably with different hubs and most presumably accepted not vindictive. Assuming any of the helpful hubs are not reacting with different hubs name as egotistical assault or remotely some other obscure hubs are entering between helpful hubs and influence the system tasks is called noxious assaults. Assault in the hubs grouped in two sorts, specifically inactive and dynamic assaults. Uninvolved assaults don't influence the system work however checked by outsider, such as spying. Where as in dynamic assaults, including bundle to invalid goal into the system, erasing parcels, and altering the course way between sources to goal may occur. In Selfish assault, a pernicious hub which assimilates and drops all information parcels and directing bundles utilizes the vulnerabilities of the on interest course revelation conventions, for example, AODV.

II. RELATED WORK

Standard Recently, a lot of research has focused on the cooperation issue in MANET. Several related issues are briefly presented here.

Khairul Azmi et al [5] present a new mechanism to detect selfish node. Each node is expected to contribute to the network on the continual basis within a time frame. Those which fail will undergo a test for their suspicious behavior. This scheme is also a based on monitor node. A monitoring node hears a request from its neighbouring node to forward a data packet; it will first check the time difference between last request and last action and status of the requestor. Performance metrics are not measures in this paper now in present work we include the infection ratio and performance metrics. Future work of [5] like acknowledgement detail and their loss are also measure.

Al Shurman et al [6] have proposed two different solutions for black hole. The first solution suggests unicasting a ping packet from source to destination through multiple routes and then chooses a safe route based on the acknowledgement received. The second solution is based on keeping track of sequence numbers. But these solutions have a longer delay and lower number of verified routes.

Misbehavior detection and reaction are described in [7], by Marti, Giuli, Lai and Baker. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission but not detect misbehavior in presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior and partial dropping. This technique is imperfect due to collisions, limited transmit power and partial dropping.

Buchegger and Le Boudec [8] present the CONFIDANT protocol. Each node monitor the behaviour of its next hop neighbors in a similar manner to watchdog. Deciding the criteria for maintaining the friends list by Trust Manager is difficult. CORE (Collaborative Reputation) [9] is a reputation based system proposed by Michiardi et alsimilar to CONFIDANT. The limitation with CORE is that the most reputed nodes may become congested as most of the routes are likely to pass through them. Also the limitations of the monitoring system in networks with limited transmission power and directional antennas have not been addressed in CORE.

[10] have proposed a collaborative architecture for black hole prevention as anextension to the watchdog method.
Bansal et al [11] have proposed a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks), which is the enhanced version of DSR protocol. OCEAN uses a monitoring system and a reputation system to identify malicious nodes. But OCEAN fails to deal with misbehaving nodes properly. These papers have addressed the black hole attack problem on unicast routing protocols.

Balakrishnan [12] has proposed a TWOACK scheme which can be implemented as an add-on to any source routing protocol. Instead of detecting particular misbehaving node, TWOACK scheme detects misbehaving link and then seeks to alleviate the problem of routing misbehavior by notifying the routing protocol to avoid them in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it cannot distinguish exactly which particular node is misbehaving node. Sometime well behaving nodes became part of misbehaving link and therefore cannot be further used the network. Thus a lot of well behaved node may be avoided by network which results in losing of well behaved routes.

Vijaya [13] proposed another acknowledgement based scheme similar to TWOACK scheme This scheme detects the misbehaving link, eliminate it and choose the other path for transmitting the data. The main idea is to send 2ACK packet which is assigned a fixed route of two hops back in the opposite direction of the data traffic route and to reduce the additional routing overhead, a fraction of the data packets will be acknowledged via a 2ACK packet. This scheme also consists of multicasting method by which sender can broadcast information of misbehaving nodes so that

Algorithm.1. False detection of selfish node for not forwarding RREQ
1: Start.
2: Source node sends RREQ to all of its one hop neighbors
3: Each normal neighbor node either rebroadcasts the RREQ to its neighbor nodes or sends an RRC packet to the sender node if it has already rebroadcasted the same RREQ before.
4: After waiting for a prefixed period of time, the source node checks its routing table and examines the behavior of its neighbors
5: IF the source node receives back the RREQ packet OR receives an RRC packet from its neighbor, THEN this neighbor node is characterized as normal node. ELSE the neighbor node is marked as potential selfish node.
6: Flooding of the RREQ continues. Each intermediate node receiving an RREQ must rebroadcast the message or send an RRC if it has rebroadcasted the same message before.

7: For each intermediate node, repeat Step2 to Step 4 and sender intermediate node is considered as the source node.
8: Process continues until destination node is reached.
9: End
Algorithm.2. False detection of selfish node for not forwarding data packets.
1: Start.
2: Initially SN is source node and RN is the 2nd node of the transmission path.
3: SN sends a Hello message to RN to confirm that RN is still present in the transmission route and updates its routing table.
4: IF SN does not receive back the hello message from RN, THEN RN is considered to be out of the transmission route and another route is established. ELSE RN is in the transmission route.
5: Data packet is sent from SN to RN. SN and RN are modified whenever data packet reaches a new intermediate node of the transmission path. Whereby the previous RN becomes new SN.
6: Step 3 is repeated with new SN and RN nodes.
7: IF new RN is out of transmission path, THEN SN sends a PB message to the previous node indicating a break in transmission path. ELSE SN broadcasts data packet to RN.
8: IF new SN does not broadcast any data packet, THEN SN is considered potential selfish node. ELSE SN is a normal node. Process continues.
9: IF SN = RN, THEN the data packet has reached the destination successfully. ELSE data packet has not reached the destination.
11: End
12: End

III. SELFISH NODE ATTACK

Routing protocols are exposed to a variety of attacks. Selfish node attack is one such attack in which a malicious node doing a routing misbehavior in the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [6,7]. This attacks aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attackers. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table and drop all the routing packets. The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious nodes do this by assigning a high sequence number to the reply packet. The attackers now drop the received messages instead of relaying them as the protocol requires. Malicious nodes take over all routes by attacking all route request messages. Therefore the quantity of routing information available to other nodes is reduced. The malicious nodes are called selfish node or nodes. The attack can be proficient either selectively or in bulk. Selective dropping means dropping packets for a specified destination or a packet every seconds or a packet every packets or a randomly selected portion of packets. Selfish attack results in dropping all packets. Both result in degradation in the performance of the network. Attacker nodes receive a request message, and send reply message to the source node. So that the source node considers the message has arrived and the communication has been successfully performed. In fact, the message did not reach the destination node
In figure 1, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a Selfish node. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D Routing in presence of Selfish node attack.

Selfish node Attack and Detection Digram

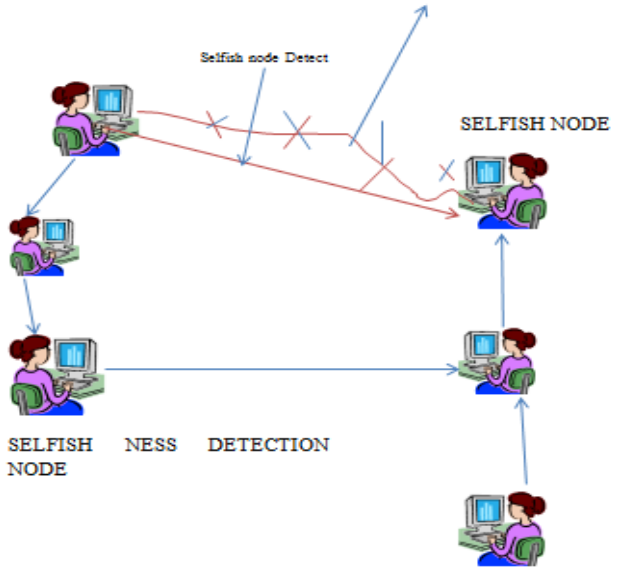

Fig 1.1 Detecting Selfish node when connection establishment

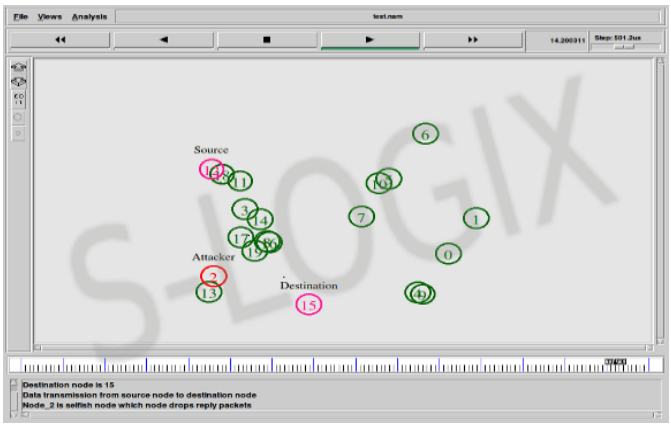

Fig 2.1 NS 2 finding selfish node attack and detecting node

IV. CONCLUSION

The normal worries in impromptu systems incorporate the entrance control: there necessities to exist a technique for confining the entrance of remote hubs to the system, which requires the utilization of a legitimate validation instrument. Additionally, the correspondence between the insider hubs in the system must be shielded from assaults on privacy. This is particularly significant in military applications, as was talked about. In the event that the connection layer does not bolster a substantial encryption plot, such instrument must be engaged with the system layer moreover. The bunch enrollment is noted in the majority of the referenced multicast conventions, however they don't recommend a particular access control or approval strategy conventions.

In Future we additionally distinguish the impact of narrow minded assault in performance matrices and furthermore Selfish hub for AODV can be executed, in actuality, situation and its analysis can be contrasted and the investigation results.

REFERENCE

[1]. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000), "Mitigating routing misbehavior in mobile ad-hoc networks", Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), ISBN 1-58113- 197-6, pp. 255-265.

[2]. S. Buchegger, C. Tissieres, and J. Y. Le Boudec. "A test bed for misbehavior detection in mobile adhoc networks". Technical Report IC/2003/72, EPFL-DI-ICA, November 2003. Available on:citeseer.ist.psu.edu/645200.html.

[3]. P. Michiardi and R. Molva. Core: "A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks",

[4]. A. Patcha and A. Mishra, "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad hoc Networks", Radio and Wireless Conference, 2003.

[5]. S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad hoc Networks", July

[6]. K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK:Preventing Selfishness in Mobile Ad hoc Networks,"

[7]. K.Vijaya "Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks,"

[8]. B. Awerbuch et al., "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures,"

[9]. S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,"

[10]. H. Yang, X. Meng, and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks,"

[11]. Moy, J. Security Architecture for the Internet Protocol. RFC 2401, November 1998, Internet Society.

[12]. Mäki, S. Security Fundamentals in Ad Hoc Networking. Proceedings of the Helsinki University of Technology, Seminar on Internetworking - Ad Hoc Networks,

[13]. Perkins, C. Mobile Ad Hoc Networking Terminology Internet draft (expired).

[14]. Gaurav Soni, "a novel defence scheme against selfish node attack in manet"

[15]. Kamlesh Chandrawansh, "a novel defence scheme against selfish node attack in manet"

