International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-5 E-ISSN: 2347-2693

Detecting Selfish node in MANET- A Review

Jagmeet kaur[1*] and Prabhjit singh[2]

[1,2]Department of Computer Science and Engineering,
Global Institute of Management & Emerging Technologies, Amritsar (PUNJAB)

Available online at: www.ijcseonline.org

Received: Apr/21/2016 Revised: May/04/2016 Accepted: May/18/2016 Published: May/31/2016

***Abstract*—** MANET (Mobile Ad-Hoc Network) is self-directed and infrastructure less network. MANETs contains mobile nodes that are free to move in the network. Nodes can be the devices like mobile phones, PDA, MP3 players and personal computers which are participating in network. MANET has the dynamic topology due to the node movement. Transmissions of the packet between the mobile devices are overcome by the Routing Protocol. Selfish node is a major problem in MANET. Selfish nodes are nodes that do not participate in forwarding process. This paper presents types of MANET protocols along with security issues that MANET faces. The major consideration of this paper is about the behavior and detection methods of selfish node in MANET.

Keywords: MANET, Routing Protocol, Security Principals

I. INTRODUCTION

During the last few years we have all witnessed a continuously increasing growth in the deployment of wireless and mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic [1].

A "mobile ad hoc network" (MANET) consists of various mobile nodes connected by wireless links. The union of which makes an arbitrary graph. In a MANET, nodes can openly move around while communicating with each other. There are two types of MANETs: open and closed. These networks build and start with the help of constituent wireless nodes. Since these nodes have only a limited transmission range, it depends on its neighboring nodes to forward packets. A node may be start working selfishly by using its limited resource only for its individual benefit; such nodes selfish cause a wide range of problems for a MANET. Congestion in a network may occur when the incoming traffic is extent than the capacity of the network. The main aim of congestion control is to lower the overall delay and reduced packet loss and offer better performance of the network which can be caused by the false node Congestion can be prevented using congestion-aware protocol through bypassing the affected links. Congestion control is the main problem in ad-hoc networks. Congestion control is associated to controlling traffic incoming into a telecommunication network.

Several nodes will be take part in the MANET for data forwarding and data packets transmission between source and destination. They must forward the traffic which other nodes sent to it. Among all the nodes some nodes will behave selfishly, these nodes are called selfish nodes [2].

II. MANET ROUTING PROTOCOL

Routing protocols define a set of rules which assign route from source to destination in a network. In ad hoc networks, topology is frequently changed, that's why nodes are not familiar with the topology of their networks. Each node learns about others nearby and how to reach them. In a MANET, there are three types of routing protocols [2]. A routing protocol is used according to the network situation.

A. Proactive Routing Protocols

Proactive routing protocols are also called as a table driven routing protocols. In these protocols every node maintains a routing table which includes information about the network topology even unless requiring it. The routing tables are updated periodically whenever the network topology changes because of the node are not fixed. Proactive protocols are not suitable for large networks because they need to maintain node entries for each and every node in the routing table of every node. Proactive protocols maintain a different number of routing tables varying from protocol to protocol. There are various routing protocols. Example: Destination-Sequenced Distance-Vector Routing (DSDV), Optimized

Link State Routing Protocol (OLSR), Wireless Routing Protocol (WRP) etc.

B. Reactive Routing Protocols

A reactive routing protocol is also known as on demand routing protocol. Reactive routing protocols do not make the nodes initiate a route discovery process until a route to a destination is required. In the Initial steps source node have to find route cache for the available route from source to destination if no route is available then node start the route discovery process. Each intermediate node involved in the route discovery process and adds latency. On demand routing protocols decrease the routing overhead but at the cost of increased latency in the network. These protocols are suitable in the situations where low routing overhead is required. Example of reactive routing protocols is: Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporarily Ordered Routing Algorithm (TORA) etc.

C. Hybrid Routing Protocol

Hybrid routing protocol combines the advantages of proactive and reactive routing. Reactive protocols have less overhead and more latency while proactive protocols have large overhead and less latency. The hybrid routing protocol is a combination of both proactive and reactive routing protocols. So a Hybrid protocol covers the limitation of both proactive and reactive routing protocols. The hybrid routing protocol uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol. Hybrid protocol is suitable for large networks where more numbers of nodes are present. This network is divided into a set of zones, where routing inside the zone is performed by using a reactive protocol and outside the zone routing is performed using reactive protocol. There are various hybrid routing protocols. Examples Zone Routing Protocol (ZRP), Sharp Hybrid Adaptive Routing Protocol (SHARP) etc.

III. NETWORK SECURITY

A security protocol for ad hoc wireless networks should satisfy the following requirements. The requirements listed below should infact be met by security protocols for other types of networks also.

A. Confidentiality

The data sent by the sender (source node) must be comprehensible only to the intended receiver (destination node). Though an intruder might get hold of the data being sent, he/she must not be able to derive any useful information out of the data. One of the popular techniques used for ensuring confidentiality is data encryption

B. Integrity

The data sent by the source node should reach the destination node as it was sent: unaltered. In other words, it should not be possible for any malicious node in the network to tamper with the data during transmission.

C. Availability

The network should remain operational all the time. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it. It should be able to provide the guaranteed services whenever an authorized user requires them.

D. Non-repudiation

Non-repudiation is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Digital signatures, which function as unique identifiers for each user, much like a written signature, are used commonly for this purpose.

E .Authentication

Enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information so it is interfering with the operation of other nodes.

IV. ISSUES AND CHALLENGES FOR MANET SECURITY

Shared broadcast radio channel: Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc wireless networks is broadcast in nature and is shared by all nodes in the network. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

A. Insecure operational environment

The operating environments where ad hoc wireless networks are used may not always be secure. One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

B. Lack of central authority

In wired networks and infrastructure-based wireless important central points (such as routers, base stations, and access points) and implement security mechanisms at such points. Since ad hoc wireless networks do not have

any such central points, these mechanisms cannot be applied in ad hoc wireless networks.

C. Lack of association

Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks.

D. Limited resource availability

Resources such as bandwidth, battery power, and computational power (to a certain extent) are scarce in ad hoc wireless networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

E. Physical vulnerability

Nodes in these networks are usually compact and handheld in nature. They could get damaged easily and are also vulnerable to theft.

V. SECURITY SCHEME

The main approach in securing ad hoc environments is the **intrusion detection approach** that aims in enabling the participating nodes to detect and avoid malicious behavior in the network without changing the underlined routing protocol or the underling infrastructure. Although the intrusion detection field and its applications are widely researched in infrastructure networks it is rather new and faces greater difficulties in the context of ad hoc networks.

A. Intrusion Detection System (IDS)

Intrusion is defined as ―any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusion protection techniques works as the first line of defense. However, intrusion protection alone is not sufficient since there is no perfect security in any system, especially in the field of ad hoc networking due to its fundamental vulnerabilities. Therefore, intrusion detection can work as the second line of protection to capture audit data and perform traffic analysis to detect whether the network or a specific node is under attack. The two types of nodes are in under attack on a network.

a) Selfish nodes

It doesn't cooperate for selfish reasons, such as saving power. Even though the selfish nodes do not intend to damage other nodes, the main threat from selfish nodes is the dropping of packets, which may affect the performance of the network severely [4].

The characteristics of selfish nodes:

- Dropping of data packets.
- Intentionally delay the RREQ packet.
- Do not replay or send hello messages.
- Do not take part in routing process.

b) Malicious nodes

It has the intention to damage other nodes, and battery saving is not a priority. Without any incentive for cooperating, network performance can be severely degraded. Once an intrusion has been detected then measures can be taken to minimize the damages or even gather evidence to inform other legitimate nodes for the intruder and maybe launch a countermeasure to minimize the effect of the active attacks[3].

VI. STAND ALONE IDS

In this architecture, each host has a IDS and detect attacks independently. There is no cooperation between nodes and all decision is based on local nodes (Fig. 1). This architecture is not effective enough but can be utilized in an environment where not all nodes are capable of running IDS.

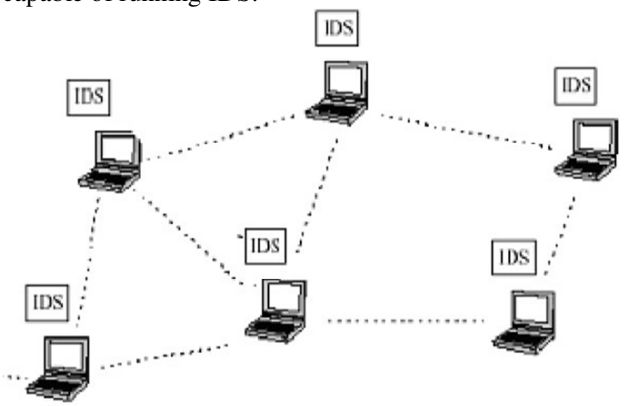

Fig. 1- Stand Alone Architecture

VII. NODE BEHAVIORAL MODEL

MANETs are mobile wireless networks that are rapidly changing, unpredictable and have no fixed base stations or infrastructure design. There are two types of MANETs: closed and open MANETs. In this case, selfish nodes are originated. These nodes will not be willing to forward packets and share their memory space for the benefit of other nodes [2]. The nodes in a mobile adhoc network can be classified into three types, such as:

A. Non-selfish nodes

These nodes allocate their memory space completely for the purpose of other nodes.

B. Fully selfish nodes

They never utilize their memory space for other nodes to store data.

C. Partially selfish nodes

These nodes may act as both selfish and non-selfish nodes. Since they have a selfish behavior, they have to be considered as selfish; rather than non-selfish. The detection of these partially selfish nodes is complex.

The major characteristics of selfish nodes include the following:

- Do not participate in routing process.
- Do not reply or send hello messages.
- Intentionally delay the RREQ packet.
- Dropping of data packet

VIII. BEHAVIOR OF SELFISH NODE

These nodes aim to get the greatest benefits from the networks while trying to preserve their own resources and use other node's resources, e.g. battery life or bandwidth. Selfish nodes attempt to maintain communications with the nodes it wants to send data packets to but may refuse to co-operate when it receives routing or data packets that it has no interest of cooperation in the network. Therefore, it may either drop data packets or refuse to retransmit routing packets that it has no interest in.

- The selfish node can do the following possible actions in Ad hoc network:
- When it receives a Route Request (RREQ), But Does not re-broadcast Route Request.
- Received Route Request (RREQ) but does not forward the Route Reply (RREP) on reverse route.
- Rebroadcast RREQ and forward RREP on a reverse route but does not forward data packets.
  - Does not unicast Route Error packets.
  - Selectively drop data packets.

IX. SELFISH NODE DETECTION METHODS

A. 2ACK METHOD

The acknowledgement-based 2ACK scheme is suggested to mitigate the adverse effects of misbehaving nodes. The basic idea of TWOACK scheme is that, when a node forwards a data packet successfully over the next hop, the next-hop-link's destination node will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. The 2ACK scheme is a network-layer technique to detectmisbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

B. S-2ACK METHOD

Another acknowledgement-based scheme, termed as S-TWOACK is a derivative of the basic TWOACK scheme, aimed at reducing the routing overhead and achieves the performance improvement along with the problem of false-alarms due to genuine TWOACK packets lost. The Selective TWOACK (S-TWOACK) scheme is different from 2ACK. Mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a change, the 2ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK scheme

C. Secure Intensive Protocol(SIP)

Secure Intensive Protocol is a credit-based method that uses the credit as the incentive to stimulate packet forwarding. Here each mobile node has a security module and they deal with the security related functions. The credits of the node increases and decreases depending on the forwarding behavior of the node. Whenever a node is initiating or forwarding a packet, first node will pass it to SIP module for processing. SIP is session based and consists of four phases, 1) Session Initiation 2) Session Key Establishment 3) Packet Forwarding And 4) Rewarding Phase.

The advantages of the scheme are SIP is:

- Routing independent.
  - It is session based rather than packet based.
- Unauthorized access is not allowed.

The disadvantage of SIP is that it implemented on hardware module so each node should possess a hardware module.

D. Core method

The reputation-based CORE (Collaborative Reputation) Mechanism to detect the selfish nodes, improves the coordination among nodes. For this purpose, it makes use of reputation mechanism and collaborative monitoring.

E. Ad-hoc vcg

Ad hoc-VCG, named after Vickrey, Clarke, and Groves is a Truthful and Cost-Efficient reactive routing protocol for mobile ad hoc networks that is robust against individual selfishness of the communication nodes and is cost-efficient. This protocol first computes the most cost-efficient path and then routes the data packets from source to destination along this path.

Ad hoc-VCG consists of the following two phases such as:

i) Route discovery.
ii) Data transmission.

Route discovery includes payment computation whereas data transmission includes the act of making payments to the intermediate nodes.
Ad hoc- VCG utilizes shortest path information to the destination node as in the case of DSR protocol. It is identical to credit-payment technique in which each node gives a credit to others, as a reward for data forwarding. This credit acquired is then used to send data to the others [3].

F. Credit Based

Credit based approach introduce the concept of money and service charges. The natural idea is that nodes that used a service should be charged and nodes that provided a service should be remunerated. To this end, introduce a node currency that we call nuggets. Now, if a node wants to use a service (send a message), then it has to pay for it in nuggets. This motivates each node to increase its number of nuggets, because nuggets are necessary for using the network. Thus, the node is no longer interested in sending useless messages and overloading the network because this would decrease its number of nuggets, and it is better off providing services to other nodes because this is the only way to earn nuggets. If node's nuggets reach at threshold value, node declares as misbehavior node.

G. Watchdog

The watchdog method allows detecting misbehaving nodes. When a node forwards a packet, the watchdog verifies that the next node in the path also forwards the packet. The watchdog listening to all other nodes within transmission range silently. If the next node does not forward the packet then it is tagged as misbehaved.

H. Pathrater

The pathrater (Rating of path), each node check possibility of every path in the network. Every node maintains a rating for every other node, it knows about the network. It computes a path metric by averaging the node ratings for the path. The calculation gives the overall reliability of different paths and allows accurate path in the network. If there are multiple paths to the same destination, path with the highest metric is more preferable.

I. Two Hop Acknowledgements:

In Two hop acknowledgment, detect misbehaving link instead of selfish node. TWOACK scheme detects misbehaving link and minimize the problem of routing misbehavior by notifying the routing protocol to avoid them for future reference. Detection of Misbehavior is dictated by sending back a TWOACK packet on successful acknowledgement of every data packet, which are assigned a fixed route of two hops (or three nodes) in the direction opposite to that of data packets.

J. Friends and Foes:

In Friends and Foes, It presents a long lived memory that allows nodes to be rewarded by services provided in the past but also does not charge by the number of hops used. The management of fairness by allowing nodes to publicly declare that they refuse to forward messages to some nodes. Every node maintains the following variables: friends, foes and selfish. The friends are the set of nodes to which node is willing to provide services. The foes are the set of nodes to which node is not willin to provide services and selfish variable gives the list of nodes which are known to act as if the node is a foe.

K. Confidant

Confidant (Cooperation of Nodes Fairness in Dynamic Ad-hoc Networks), has four interdependent modules monitor, reputation system, path manager and trust manager. First monitor collects evidence by monitoring the transmission of a neighbor after forwarding a packet to the next node in the route. Then reports to the reputation system only if the collected evidence represents a malicious behavior in the network. Reputation system changes the rating for a node if the evidence collected for a node's malicious behavior greater than the predefined threshold value. Then, path manager makes a decision to delete the malicious node from the path. Provide and accept routing information, accept a node as a part of route, and take part in a route originated by some other node this kind of Decision will take by Trust manager.

	Observation		Detection		Punishment
	Self to Neighbor	Neighbor to Neighbor	Selfish Node	Selfish Routing	
Credit Based	Yes	No	Yes	No	Ye
Watchdog	Yes	N	Yes	No	N
Pathrater	Yes	N	Yes	No	N
Two ACK	Yes	Yes	Yes	Yes	No
Friend and Foes	Yes	No	Yes	No	Ye
Confidant	Yes	N	Yes	Yes	Y

Table 1- Comparative study [5].

X. CONCLUSION

One of the problems in MANET is the presence of selfish nodes in the network which could seriously degrade the network performance. Behavior of selfishness is appearing frequently in MANET. Due to the selfishness of node performance parameter were decreasing. This survey paper discussed selfish node attack and different techniques related to detect selfish node. The detection and removal of selfish node must be done in order to improve the network performance. Detection of selfish node can be done easily and effectively by introducing clustering mechanism.

REFERENCES

[1] Dipali D. Punwatkar and Kapil N. Hande, "A Review of Malicious Node Detection in Mobile Ad-hoc Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-02, Page No (65-69), Feb -2014

[2] Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani and Kamal Bunkar, "An Overview & Study of Security Issues in Mobile Ado Networks", International Journal of Computer Science and Information Security (IJCSIS) USA, Vol-9(4), pp (106-111), April 2011

[3] ayank Kumar and Tanya Singh, "A Survey on Security Issue in Mobile AD-HOC Network and Solutions", International Journal of Computer Sciences and Engineering, Volume-02, Issue-03, Page No (71-75), Mar -2014

[4] M.Madhumathi, S. Sindhuja, " A Survey on Collaborative contact-based Selfish node detection in Mobile ad hoc Network", International Journal of Advanced Research in Computer Engineering & Technology, Volume 4 Issue 10, October 2015

[5] Nikunjkumar Varnagar, prof. Amit Lathigara, "Review Paper of Selfish Node Detection in MANET", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 2, February 2015

[6] G.Satyavathy and P. Anitha, "A Collaborative Contact-Based Watchdog CoCoWa for Detecting Selfish Nodes with Trust Model", International Journal of Computer Sciences and Engineering, Volume-03, Issue-09, Page No (120-123), Sep -2015

