IJCTA, 10(02), 2017, pp. 79-84

Survery Over the Detection Selfish Nodes in Manet

Anitha T* Nalina E and John Justin Thangaraj****

Abstract : The Mobile Ad hoc Network (MANET) is multi-hop in nature wherein every node transfers information packets to different nodes. It is a system intended to work adequately over extraordinary separation. However because of security defenselessness, the system faces genuine risk, and attacks. These Misbehaving nodes may affect the network working causing performance delays. Any system that are connected to the network will be prone to some unauthorized data as it do not check the users authenticity to access the data. Wireless network like MANETS are vulnerable to attacks than compared to wired networks. This paper concentrates on different attacks, and the detection method for misbehaving nodes in the network.

Keywords : Detection, Attack, MANETS.

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) is an effective field in the advance of Wireless system. It utilizes dynamic topology, remote connections, decentralized system and needn't bother with any focal foundation. MANET is a framework less, dynamic system. It comprises of gathering of remote portable hubs, and the correspondence between these hubs. They could be more prudent at times as they dispense with settled framework costs and decrease control utilizations at portable hubs.

We can categorize nodes into 3 ways namely :

Malevolent nodes : Hubs that need to trade off the security of the MANET or of different hubs. Their activities are coordinated on some sought impact, yet they are for the most part not reasonable on the grounds that they don't make progress toward their own particular benefit amplification.

Selfish nodes : Hubs that don't forward other's bundles, in this manner boosting their benefit to the detriment of all others. They are expected to dependably act judiciously, so they cheat just on the off chance that it gives them favorable position.

Erroneous nodes : These are nodes with failing hardware or incorrect software. They do not intentionally misbehave but if they impair the working of the net, then they have to be treated just as malevolent.

A selfish node is one that tries to use the system assets for its own benefit yet is hesitant to spend its own for others. On the off chance that such conduct wins among huge number of the hubs in the system, it might inevitably prompt to interruption of system. This paper ponders the effect of narrow minded hubs fixation on the nature of administration in MANETs.

The characteristics of selfish nodes are :

1. No participation in routing process: A selfish node changes the route request and reply messages.

* PG Scholar, VeltechMultitechDr.RR& Dr.SR Engineering College, *anitsept@gmail.com*

** Assistant Professor, VeltechMultitechDr.RR& Dr.SR Engineering College, *nalinasmit@gmail.com, johnjustin.er@gmail.com*

2. Donot reply or send hello messages: A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it
3. Intentionally delay the RREQ packet: A selfish node may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths.
4. Dropping of data packet: A selfish nodes may participate in routing messages but may not relay data packets.

Routing Algorithm In Manets

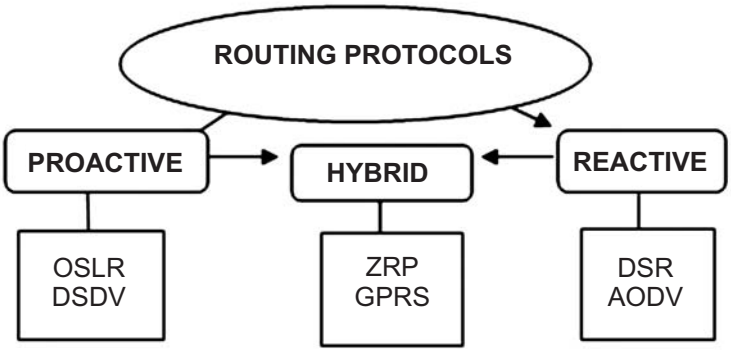

Figure 1

Proactive Protocol

In proactive protocol each node in the system has at least one route to any possible destination in its directing table at any given time (*i.e*) every one of the nodes persistently look for routing data with in a network. This protocol exhibits low inactivity but medium to high directing overhead. This is because of the nodes occasionally exchange control messages and directing table data with a specific end goal to stay up with the latest courses to any dynamic node in the system. Proactive protocol can better address security vulnerabilities, due to the intermittent trade of control messages and continuous upgrade of the routing data. The two commonly known proactive protocols, are Optimized Link State Routing (OLSR) and destination sequenced distance vector (DSDV).

Hybrid Routing Protocol

The Hybrid protocol is the mix of proactive and reactive protocol. The zone territory that is inside the required district or the limit ,the nodes are gathered into zones in view of their topographical areas or separations from each other. In the event that the required routing as to be done in a short separation it is done utilizing table-driven instruments (*i.e*) Proactive protocol while if the locale goes past the directing territory it is finished by on-request routing (*i.e*) Reactive for protocol. Examples of hybrid protocol are ZRP (Zone Routing Protocol), GPSR (Greedy perimeter stateless routing).

Reactive Protocol

The reactive protocol is likewise called as On Demand Routing Protocols where the courses are not known before for the directing reason. A node which needs to convey the information exchange to another node (destination),where it is inaccessible. The source node requires the course disclosure stage to decide another course at whatever point a transmission is required. Reactive strategies have littler routing overheads yet higher latency. Example Protocols**:** DSR, AODV

Route Discovery

This route discovery mechanism depends on flooding method which utilizes on the system that a node just communicates by sending to its neighbors and intermediate nodes simply forward packets to their neighbors.

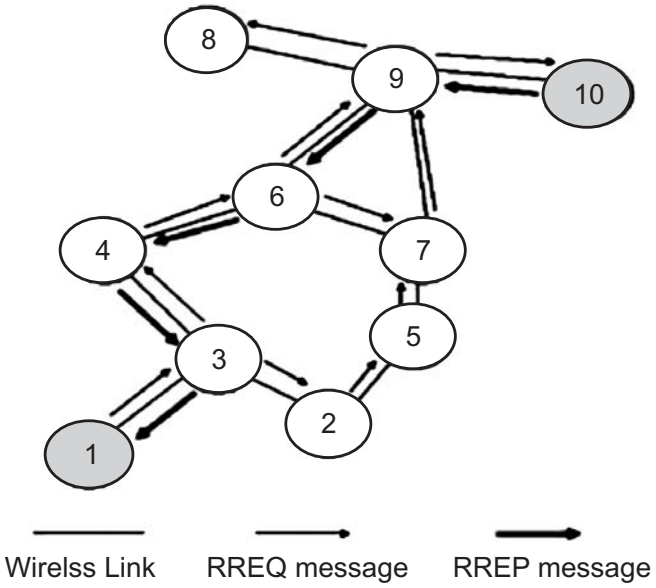

Figure 2: Flooding algorithm

This is a repetitive technique until it reaches the sink.

2. ATTACKS IN MANETS

Providing security to mobile ad-hoc networks is most common challenge in the network. Knowledge of the possible vulnerabilities,attacks and their effects in the network is the basic step of security. Security of communication in MANET is important for secure transmission of information. There are number of attacks that affect MANET.

2.1. Classification Based On Location

Security attacks can be mainly categorized into Internal and External. External attacks are on the basis of Location.

1. Internal Attack:Internal attack is the one that are from a node ornodes that are within the network. The malicious nodes or misbehaving nodes inside the network willbroadcast incorrect routing informationto other nodes in the network,there by affecting the normal functioningof the network. Internal attacks are hard to detect as thecompromised nodes are capable of generating valid digitalsignatures using their private keys.
2. External Attack:External attack is the attack that is from a nodeor nodes that don't belong to the network. They can causenetwork congestion, unavailability of network services andalso produces additional network overhead therebypreventing the network from information exchange.

2.2. Classification Based On the Nature of Attack

1. **Passive Attack :** In passive attack, the attacker does not misuse the information exchanged but listens to it. They try to acquire confidential information and analyze the traffic

   Patterns transmitted. They are hard to detect as they do not interrupt or modify the data being sent or received.
2. **Active Attack :** In Active attack, the attacker actively participates in the network activities andtries to change the messages being broadcasted. The attacker will change,inject, forge, fabricate or drop data packets by disturbing the whole network. The result of this attack is high as they bring down the entire network. They are easy todetect as the network performance decreases significantly.

2.3. Attack Classification on Different Layers

(*a*) Selfish misbehavior of nodes : These are selfish nodes that either deny sending the packets or drop the packets deliberately with a specific end goal to retain battery power or increases undesirable share of transmission capacity. Packet dropping is one of the significant assaults by selfish node which causes congestion in system. These attacks exploit the routing protocol to their own advantage because most of the routing protocols have no mechanism to detect whether the packets are being forwarded or not except the Dynamic Source Routing protocol.

(*b*) Malicious behavior of nodes : They disrupt operation of routing protocol and its effectwill be considerable only when more communicationtakes place between neighboring nodes.

(*c*) Traffic Analysis : In this type of attack the attacker has the knowledge of trafficpatterns to know important information on networktopology that reveals the information about the nodes. Information such as location of nodes, networktopology used to communicate and roles played by thenodes can be gathered.

(*d*) Denial of Service (DoS) Attack : A denial-of-service attack is an attempt to make the network resource unavailable to itsIntended users, such as to temporarily or indefinite interrupt or suspend services of a host connected to the Internet. This attack can be launched at network layers, by signal jamming attack where the normal communication is disturbed, a malicious nodes take hold of the channel and prevent other nodes from channel access, DoS attacks are launched on routing protocols to degrade the network performance by adding different routing packets.

(*e*) Worm hole attack : In the wormhole attack, a selfish node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By this shortcut, they could trap the source node to know the route discovery process and later launch the interception attacks. Packets from these two connections are created for the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently do not allow other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations.

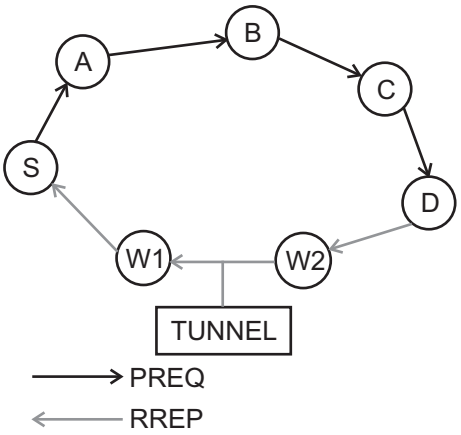

Figure 3

W1 and W2 are the attacker included that can either drop packet or drop packets selectively to avoid detection.

(*f*) Black hole attack : In this attack, malicious nodes tracks all their neighboring nodes to know about the routing packets to them. As in the wormhole attacks, selfish nodes could launch the black hole attacks by broadcasting themselves to the neighboring nodes as having the most optimal route to the requested destinations.

However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its

neighboring nodes. The attacker pretends to be a new node and sends a fake response as reply to the source S, when the actual hop count to reach the destination is 5.

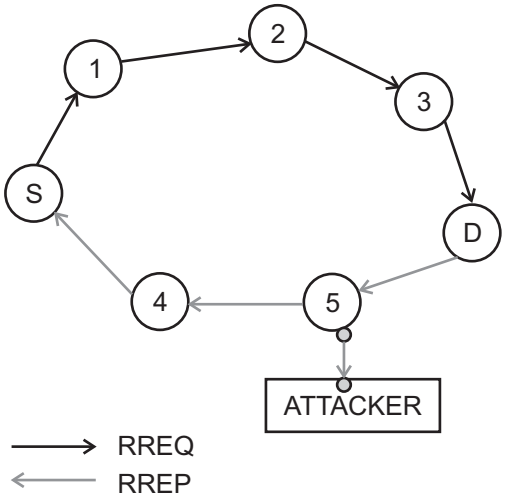

Figure 4

(*g*) Gray hole attack : Gray hole attack is similar to Black hole attack with a small difference. The attacker sends fake message to source (or victim) node as in Black hole attack but it doesn't drop all the data packets. It drops few selective packets and forwards the rest of them. This attack is relatively difficult to detect as it drops some selective packets and forwards the rest. This situation can bemistaken for network congestion or some other valid reason.

(*h*) Node isolation attacks : The goal of this attack is to isolated a node from communicating with other node in the network more specifically this attack prevent the victim node from receiving data packets from other node in to the networks. In these attacks the attackers prevent link information of a specific node, the group of nodes. From being spread to the entire network. Those other node which could not receive the link information of the target node will not be able to build a route to the destination node and hence will not able to send data packets to these nodes.

3. SELFISH NODE DETECTION

In this section we will describe the methods to detect the selfish nodes in the network:

Pathrater Module

The pathrater, keep running by every hub in the system, joins learning of getting out of hand nodes with connection unwavering quality information to pick the course well on the way to be solid. Every hub keeps up a rating for each other hub it thinks about in the arrange. It figures a way metric by averaging the hub appraisals in the way. We pick this metric since it gives an examination of the general dependability of various ways and permitspathrater to copy the most limited length way calculation at the point when no unwavering quality data has been gathered, as clarified underneath. In the event that there are different ways to the samegoal, we pick the way with the most elevated metric. Take note of that this varies from standard DSR, which picks the most limited way in the course reserve. Assist take note of that sincethe pathrater relies on upon knowing the correct way a bundle has navigated, it must be actualized on top of a source steering convention.

The pathrater doles out appraisals to hubs as indicated by the accompanying calculation. At the point when a hub in the system gets to be known to the pathrater (through course revelation), the pathrater allots it an "impartial" rating of 0.5. A hub dependably rates itself with a 1.0. This guarantees while computing way rates, if every other hub are nonpartisan hubs (instead of suspected getting out of hand hubs), the pathrater picks the most brief length way. The pathrater increases the evaluations of hubs on all effectively utilized ways by 0.01 at occasional interims of 200ms.

An effectively utilized way is one on which the hub has sent a parcel inside the past rate increase interim.The most extreme esteem an impartial hub can accomplish is 0.8. We decrement a hub's appraising by 0.05 when we identify a connection break amid bundle sending and the hub gets to be inaccessible. The lower bound rating of a "nonpartisan" hub is 0.0. The pathrater does not adjust the appraisals of hubs that are not right now in dynamic utilize.

Watch Dog

The identification of Watchdog convention is present. In this convention, each hub is work as an onlooker to watch the working of its next trust neighborhood hub. It gathers transmission data of this hub and watches that hub accurately forward to its next trust neighborhood hub alongside the right goal route.This convention measures the sending time of the following trust hub. In the event that the sending time of the following jump neighbor is more noteworthy than the parcel putting away time and surpasses over some characterized edge of the system, then Watchdog realizes that framework is under dark opening assault and it instantly stamp this hub as a pernicious hub. The Watchdog convention reports the presence of the malevolent hub in the system by producing the cautions. The advantage of the Watchdog convention is that, they make utilization of just nearby data and are capable to recognize the noxious hub. They can resolve the dilemma of dark opening assault which exhibit the best approach to dissent of administration assault (DOS) in MANET organize.

Guard dog convention go about as a decent interruption location framework instrument in the system. In any case, there are sure inconveniences in regards to this convention to such an extent that it diminishes the system execution as far as throughput, it doesn't bolster versatility with high number of hubs, and it doesn't recognize the genuine reason of the bundle misfortune. To beat these hindrances of this Watchdog convention, the enhanced Watchdog system is proposed which superbly recognizes the parcel misfortune because of clog or because of the nearness of a malignant hub in the system. Our enhanced Watchdog convention additionally bolsters a high level of the versatility and improves the execution.

4. CONCLUSION

Here by we can conclude that there are so many attacks are possible in the network and the selfish behavior of the nodes leads to such attacks. Each attack based on location, nature or the layers has serious effect in the network. Each attack has different approach to arrive the solution.Initially fuzzy logics used to predict the nodes behavior but now using Geographic routing protocol data is retrieved securely from the current location. The idea of iTrust is to introduce the trust authority periodically for probabilistic checking each zone's forwarding evidence in dynamic environment.

5. REFERENCES

1. Saritha Reddy Venna, Ramesh BabuInampudi" A Survey on Security Attacks in Mobile Adhoc Networks", International Journal of Computer Science and Information Technologies, Vol7(1),2016.
2. ShailenderGupta C, Nagpal K, CharuSingla "Impact Of Selfish node Connection in Manets", International Journal Of Wireless & Mobile Networks (IJWMN) Vol.3, No.2,April 2011.
3. M.Madhumathi, R.Ashok Kumar " Selfish Node Detection in Mobile Ad-Hoc Networks through Audit Approach with Correlation Function",International Journal of Computer Science Trends and Technology (I JCS T) – Volume 4 Issue 3, May - Jun 2016.
4. K.P Manikandan, Dr.RSatyaPrasad "A Survey on Attacks and Defence Metrics Of Routing Mechanism in Mobile Ad Hoc Networks" International Journal of Advanced Computer Science and Applications,Vol. 2, No.3, March 2011
5. Prof. MasrathBegum,Nithesh S.P, "Secure Manets from DOS Attack Using EOLSR",International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 7, July 2014.