A Review Paper on Behavior of Node in MANET

Vaibhav V. Bhujade[1]
Department CSE
DMIETR
Wardha, Maharashtra
bhujadevaibhav@gmail.com

Deepak Chaudhary[2]
Department of CSE
IET
Alwar, Rajasthan
deepak.se17@gmail.com

Suraj V. Raut[3]
Department of CE
BDCE
Wardha, Maharashtra
surajvraut@gmail.com

***Abstract* -** MANET Mobile ad-hoc networks (MANETs) is wireless network composed of various wireless equipment connected without any pre-existent infrastructure. It connects various types of equipment through wireless networking. But whenever this network has to communicate with other system it takes the help of its neighbor to send the data so it needs the corporation from other nodes of the network. Also when any node is no relation with the sending data it acts as a medium to forward the unrelated traffic. This is the ideal condition which is expected but in real world most nodes may have selfish behavior who are not corporate to forward the packet to save the resource. So in this paper we are going to study of the selfish node in MANET & their behaviors in various aspects.

Index Terms—*MANET, selfish nodes*

*****

I. Introduction

Opposed to the infrastructure wireless networks where each user directly communicates with an access point or base station, a mobile ad hoc network, or MANET is a one of the kind of wireless ad hoc network. It is a self-connecting network of mobile routers connected by wireless links with no access point. Every mobile device in a network is separate in their own way. The mobile devices are free to move to anywhere and organize themselves arbitrarily.

In other words, ad hoc network do not rely on any fixed infrastructure (i.e. the mobile ad hoc network is infrastructure less wireless network. The Communication in MANET is done by using multi-hop paths network. Available nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, distortion in communication link is very frequent, as nodes are free to change their position to anywhere. The density of nodes and the number of nodes are depends on the applications in which we are using MANET. [2]

Usually, it is expected that all nodes forward as per requirement, but other decided policies are possible as well (e. g. only require forwarding as long as a node's battery level is on high level). In any other way the MANET's protocols and policies imply a normative expectation on every participating node

a) to behave according to agreed protocols and

b) to forward a fair amount of other node's packets as needed

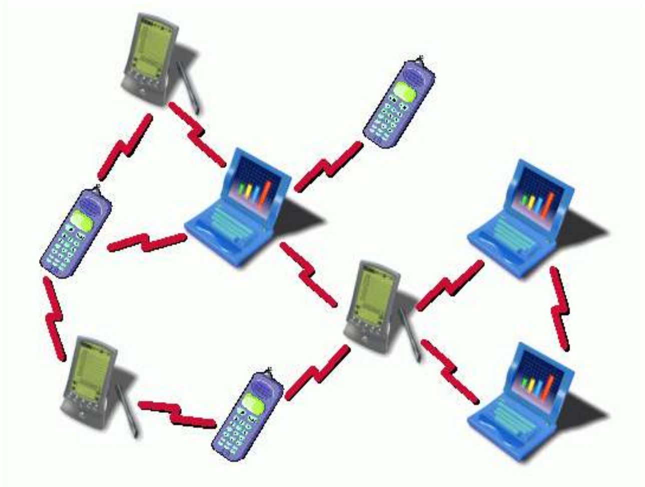

Fig. 1 of MANET Network

MANETS are used in various contexts like intelligent transportation systems, mobile social networks, emergency deployment, etc. In a MANET, nodes can freely move around while communicating with each other. These networks may be in the under-perform in the presence of nodes with a selfish node behavior, particularly when nodes operating under energy constraints. A selfish node will not cooperate in the communication, data sending, transmission of packets, badly affecting network performance. Also, nodes may also fail to cooperate either intentionally (a malicious behavior) or due to faulty software or hardware. [1]

As there is no dedicated infrastructure or central coordination, the nodes have to cooperate and self-organize to form a working communication network. Communication only works if nodes participate and forward other node's packets. On the other hand every node has to consider its limited resources (most notably its energy). So every node is motivated to contribute as little as possible of its own energy. Usually, it is expected that all nodes forward as per requirement, but some more policies are possible as well (e. g. only require forwarding as long as a node's battery level is high). In any way the MANET's protocols and policies imply a normative expectation on every participating node a) to behave according to agreed protocols and b) to forward a fair amount of other node's packets as needed. [3]

As long as all nodes adhere to this and cooperate, the MANET should work without any difficulties. One of the most important issues in designing MANET protocols is how to deal with nodes that do not cooperate. Depending on their (or their user's) motivation I will categorize these nodes into three groups:

- Malevolent nodes – Nodes that want to compromise the security of the MANET or of other nodes. Their actions are directed on some desired effect, but they are generally not sensible because they do not strive for their own benefit maximization.

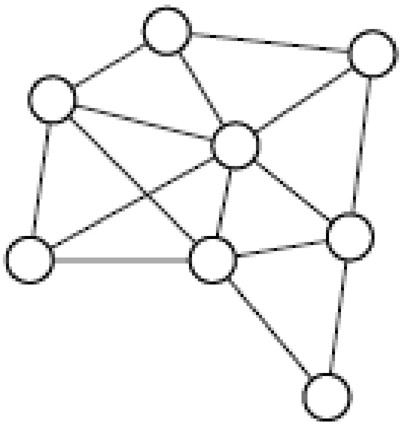

Fig. 2. A highly connected net

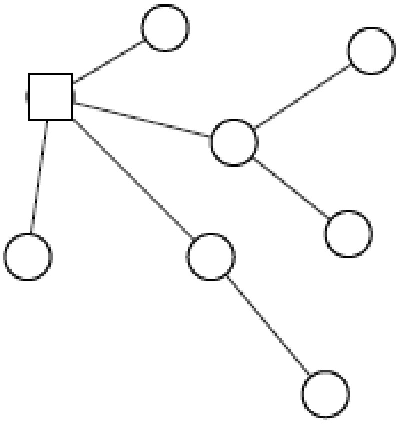

Fig. 3. A hybrid net degraded ino a tree

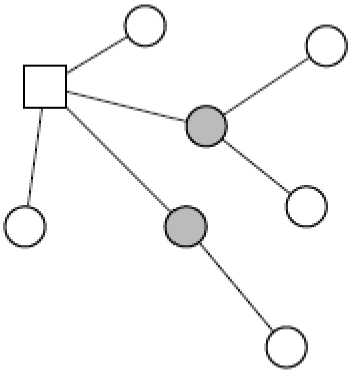

Fig. 4. A hybrid MANET with routes to/from the gateway: very few nodes (grey) actually have to forward other nodes' data.

- Selfish nodes – Nodes that do not forward other's packets, thus maximizing their profits at the expense of all others. They are assumed to always behave rationally, so this node cheat only if it gives them an advantage.
- 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 or selfish nodes.

Cryptography and Security

Most techniques presented here need cryptographic algorithms in order to be securely and reliably implemented. A basic understanding of symmetric and asymmetric (or public key) encryption, key chains, message authentication, digital signatures, and threshold cryptography are useful to appreciate the possibilities and consequences of these methods.

In order to define attacks a traditional understanding of host and network security is presumed as well. A system is considered secure if it ensures confidentiality, integrity, security, provide protection against masquerade, availability, and accountability of all actions. Any action that assaults this security is considered an attack. [3]

II. NODE MISBEHAVIORS IN MANETS

MANET naively assume that all the nodes in the network are cooperative in performing the networking tasks. This can be guaranteed if all of the nodes belong to a single authority where all of them have the same common objective. However, that is not the case such as in civilian used applications, some of these present nodes may behave selfishly and only act towards those that add to their own benefits. Providing network services such as forwarding packets and detecting routes consumes network bandwidth, local CPU time, memory and battery power which are limited in MANET nodes. For example, simulation studies show that when the average numbers of hops from a source to a destination is around 5, then almost 80% of the transmission energy will be devoted to packet data forwarding. By denying services for others nodes, a node could reserve its resources for its own use and stay longer in the network. So there is a strong motivation for the nodes not to cooperate and misleading. In general, there are two types of node misbehaving: [3]

I) MISLEADING :

A misleading node is selective in choosing which packet it wants to respond. It behaves like an honest node in a network, responding to all control received packets during route discovery process. However when the node receives a data packet to be further forwarded, the misleading node silently leave it. The reasons for choosing data packets for dropping is because data packets are generally greater in term of size and number than the control packets and thus consumes more energy to forward packet and data. This type of behavior of any node is also called “Gray Hole Attack”.

II)SELFISH :

Selfish node aims to save its resources to the maximum. This type of misbehaving node delete all incoming packets (control and data) except those which are appoint to it. By falling control packets, the nodes would not be included in the routing and then be released from being requested to forward data packets. The similarity of these two types of misbehaving is that they both use the network to forward their own packets but refuse to provide the same services back. Misbehaving nodes can significantly take down the performance of a MANET. Simulation shows that the percentage of misleading nodes can decrease the number of packets that are successfully delivered in the network. When 50% of the nodes of the network become misleading, the packet delivery ratio (PDR) degrades by 55%. Selfish nodes on the other hand, have no big effect on PDR. However, this type of non-corporation can increase the average end to end delay. As the number of count of selfish nodes been increased, the sender node will have very less option on which route the data packets should use for travelling. As a result, less feasible route will be selected which means longer delays. It also means that the all other cooperative nodes have to take the extra burden of forwarding packets. If 50% of the nodes become selfish, the average end to end delay increases by 60%. [4]

Passive Attacks

1) Eavesdropping: The simplest attack on a wireless net is eavesdropping; it requires minimal preparation and cannot be detected. Eavesdropping can be subdivided as follows:

1) The content of communication. As there exist various techniques to encrypt the content, guaranteeing its confidentiality is not difficult. As encryption is an expensive operation users of mobile clients might choose not to encrypt in order to save computing and energy resources.

2) Infrastructure meta-data, including used protocol options and especially routing information. Encrypting this communication is possible, but usually not worth it because it would require sophisticated key management among the participants.

3) Amount and distribution of communication or location of node. Even without knowing any content, an eavesdropper can still detect traffic patterns among the nodes. In theory this could be avoided by randomly sending messages between nodes but in mobile environments this is infeasible due to energy constraints. Depending on the MANET’s use and policy even the disclosure of a node’s location might be considered a successful security breach.

2) Non-Participation: After joining the MANET a node could simply refuse to forward other node’s data. There are two alternatives:

1) The node does not respond to route request messages. – This is a selfish behaviour but it does not impair the net as it will find another (maybe suboptimal) route.

2) The node does respond to route request messages, but when becoming part of a route it silently discards the data it is supposed to forward. – This works well because all nodes are supposed to forward data, but most nodes are at the perimeter and only few nodes are actually part of used routes inside the net (cf. Fig. 3).

Active Attacks

• Denial of Service. With enough resources an attacker can always send more data than other nodes can process. Mobile clients are especially vulnerable to denial of service attacks because it quickly drains their energy reserve. Another possible approach does not even need to send large amounts of data but just sending enough packets to prevent a node from going into sleep- oder energy saving-mode; this is called sleep deprivation.

• Manipulate forwarded data. This is an potentially dangerous attack but quite simple to prevent by using message authentication.

• Manipulate routing meta-data. – Simple denial of service – some routing protocols allow very simple attacks, like sending data for non-existing node targets, thus creating a node route-finding broadcast.

– Black hole – a node can announce itself as having the shortest path to all other nodes, thus it disrupts existing routes and attracts much traffic. Getting a large amount of data leads to new opportunities like selectively forwarding/dropping packets (sometimes called grey hole) or various kinds of traffic and content analysis.

– Wormhole – collaborating attackers can create two or more black holes and connect them (out of band, e. g. by directional antennae or wire). This gives them control over large parts of the MANET and its packets.

– Eclipse – collaborating attackers can partition the net, thus controlling all data flowing between the partitions. Depending on the number of attackers one can separate single nodes, get between a base station and its clients or even bipartition a large net.

HYBRID MANETS

Some advantages of a hybrid MANET, i. e. a MANET with one or more fixed base stations.

• Base stations can act as gateways into wired nets, usually providing access to the Internet. This also makes them the most suitable places for traditional intrusion detection systems.

• Multiple base stations can be connected by directed antennae or wired net, thus forming a backbone and enlarging the range of the MANET.

• Base stations can simplify the routing, e. g. by keeping track of all participating nodes.

• Base stations can act as a CA, key server, clearinghouse, or other trusted instance for distributed processes.

As a secondary effect MANETs with gateways often have different traffic patterns. Instead of the archetypical MANET with every node communication at random with all other nodes, a MANET with gateway can have a very simple communication structure with all nodes only talking to the gateway. In this case the fully connected net degraded into a spanning tree with the gateway as its root. If this is expected, then the routing becomes substantially simpler – every packet can be forwarded up to the root and then down to the receiving node.

On the other hand fixed base stations raise the problem of Single Points of Failures – all advantages are lost if a MANET has to rely on a single base station. Thus a hybrid MANET structure should always have various redundant base stations and if the net is important then the base stations themselves should use only redundant resources (i. e. if they act as gateways they should have two different Internet uplinks using different switches, if they act as a clearinghouse they should use a highly available database).

III. CONCLUSION

Many explicit or implicit requirements on MANETs are mutually exclusive. Implementing such a net always requires decisions and trade-offs. Probably the most important decision is weather to require fixed identities, since a number of protocols rely on this for accountability and recognizability of participants and their actions. The very basic properties of wireless communication and the necessary self-organization of MANETs lead to some weaknesses that can be abused for attacks. Even with mature and security-aware protocols it is very hard to mitigate this kind of attacks as the trade-offs might be too big (always considering the limited resources of mobile devices). Besides security considerations it is just as essential to create incentives for node cooperation, as the net has to rely on it.

Many protocols were suggested to enforce cooperation and as to detect misbehaving nodes. All of them make certain premises which make them more suitable for some scenarios and less suitable for others. As only few of them are actually implemented their evaluation is mostly based on simulations and there is no first-hand experience on their effect on real and sufficiently large MANETs.

IV. REFERENCES:

[1] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, " Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog" in IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 5, MAY 2012

[2] Mohit Kumar & Rashmi Mishra, "An Overview of MANET: History, Challenges and Applications in Mohit Kumar et al / Indian Journal of Computer Science and Engineering (IJCSE)

[3] Martin Schütte, "Detecting Selfish and Malicious Nodes in MANETs" in Detecting Selfish and Malicious Nodes in MANETs

[4] Sagar D. Padiya, Rakesh Pandit, Sachin Patel "A System for MANET to Detect Selfish Nodes Using NS2" in International Journal of Engineering Science and

Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012

[5] S. Buchegger, "Coping with misbehavior in mobile ad-hoc networks," Ph. D. Thesis, EPF Lausanne, Apr. 2004. [Online]. Available: http://www.sims.berkeley.edu/~sonja/phdThesis.pdf

[6] P. Michiardi, "Cooperation enforcement and network securitymechanisms for mobile ad hoc networks," Thesis, Ecole Doctorale d'Informatique, Télécommunications et Électronique de Paris, Dec. 2004. [Online]. Available: http://pastel.paristech.org/ archive /00001114/

[7] A. Urpi, M. Bonuccelli, and S. Giordano, "Modelling cooperation in mobile ad hoc networks: a formal description of selfishness," in WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003, INRIA Sophia-Antipolis, France, 2003.

[8] G. F. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: a survey," Wireless Communications and Mobile Computing, vol. 6, no. 3, pp. 319–332, 2006.

[9] A. Weyland, "Cooperation and accounting in multi-hop cellular networks," Inauguraldissertation, Universität Bern, 2006. [Online]. Available: http://www.iam.unibe.ch/~rvs/research/ pub_files/ We05.pdf