International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182 Print ISSN: 2349-5979
www.allsubjectjournal.com
Volume 2; Issue 12; December 2015; Page No. 90-93

Exponential consistency count based reputation mechanism in Manet's

[1] Bala Subramanian R, [2] Madhavan P, [3] Keerthana G

[1] Department of computer science and engineering, Sri Krishna college of Technology

[2] Department of computer science and engineering, Sri Krishna college of Technology

[3] Department of computer science and engineering, Sri Krishna college of Technology

Abstract
This paper provides the energy efficient to identify the selfish node at the time of packet transmission. In MANET, packets are routed from one node to another node through intermediate nodes for communication purpose. The intermediate nodes can act as selfish behavior and will not transfer or forward the packets to neighbor node, thus it save its resources by itself. Thus the overall routine of the network will get pretentious. Watchdog mechanism used t detect the selfish node sometimes leads to failure and it produce a wrong information to the system. The use of watchdog leads to poor performance when detecting the selfish node in terms of speed and precision. Thus we propose an augmented consistent count based mechanism to evaluate the behaviour of the different mobile nodes. From the replication result, the offered approach Energy based selfish node detection terms of performance evaluation metrics such as delay, packet loss, throughput, packet delivery value and overhead. Further this mechanism has a reasonable rate of 20% in isolating the selfish node from the routing path.

Keywords: MANET, Selfish node, watchdog

1. Introduction
The two types of wireless network are infrastructure and infrastructure less network. In infrastructure wireless network, base stations are fixed. Nodes moves randomly in the wireless environment and node communication takes place with the help of base station. It acts as the central controller, which controls the network functions effectively. Examples of infrastructure wireless network are cellular phone and paging systems. It can efficiently utilize the network resources for controlling the activities like transmission scheduling, dynamic resource allocation and power control. But, it is more exclusive or simply not achievable or practical to organize infrastructure. Infrastructure less wireless networks is also called Adhoc Wireless Networks, in which separately node participates in routing by forwarding data for other nodes, so the purpose of which nodes forward data is made vigorously on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use overflowing for promoting data. MANET is self-organizing and adaptive which enables user to communicate without any physical infrastructure. Device should be able to detect the presence of other devices which performs necessary set up to facilitate communication and sharing of data and service. It allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Figure 1 shows a simple ad-hoc network.

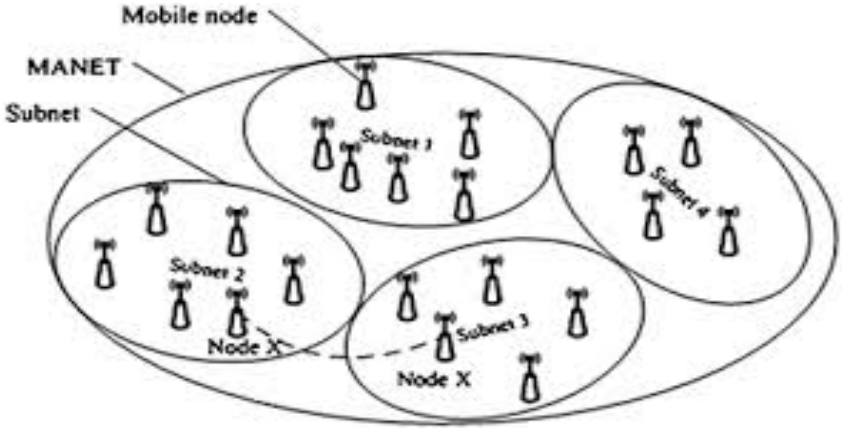

Fig 1

The collaboration on these networks in MANET is usually communication based. Mobile nodes can directly communicate with each other if a contact happens (i.e., if they are inside communication range). Supporting this cooperation is a cost intensive action for mobile nodes. Thus, in the actual world, nodes could have a selfish behavior, being unwilling to onward

packets for others. Selfishness funds that some nodes unused to forward other nodes' packets to save their own resources. The literature provides two main strategies to deal with selfish behavior: a) motivation based approaches, and b) discovery and elimination. In proposed, we do not attempt to implement any strategy to exclude selfish nodes or to incentivize their participation; instead, we focus on the detection of selfish nodes.

2. Related Works

2.1. Securing MAODV: Attacks and Counter Measures

MAODV does not contain any supplies for security; thus, it is susceptible to attacks by outsiders as well as malicious insiders. Many bouts on routing conventions for ad hoc networks have been described in the literature. Attackers may drop, modify, replay or fabricate routing messages. Nodes may also impersonate other nodes while sending fabricated messages. Additional, numerous attacker nodes may connive to take-off attacks, e.g. wormhole attacks. In general, attacks on MAODV can be divided into two classes: (i) attacks on route detection and creation, (ii) attacks on multicast tree maintenance. The route detection and creation protocols for MAODV are similar to the protocols used in AODV.

The attacks on these practices in MAODV are like to the attacks on AODV that have been conversed in the poetry. In contrast, the attacks on the multicast tree development and maintenance in MAODV have no counterpart in uncast routing protocols. We define below numerous attacks on the operation of MAODV. Each attack has a two-part name - the initial part states which message (e.g., RREP) or which property (e.g., group leadership) is distorted to launch the attack, and the second part indicates the result of the attack, e.g., panel in the multicast tree. For brevity, group guidance is abbreviated as G, divider in the multicast tree is shortened as PART, invalid route as INV and multicast tree creation as MTF. To launch an attack, if the communication changed (e.g., MACT) includes a special flag (e.g., Join flag J), the communication name includes the flag in asides (e.g., MACT (J)).

2.2. Faces: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANET Systems

Sanjay K. Dhurandher *et al* [1], proposed the Friend based Ad hoc directing using Experiments to Establish Security (FACES) is an algorithm to provide locked routing in ad hoc mobile networks. The algorithm works by transfer meets and sharing friends Lists to deliver a list of consistent nodes to the source node complete which data communication to finish takes place. The nodes in the friend list are evaluated on the basis of the total of data communication they complete and their friendship with other nodes in the system. The account of friendship of a node with other nodes in the network is acquired through the Share Your Friends method which is a broken event in the network. As a result of this structure of operation, the network is able to effectively isolate the malevolent nodes which are left with no character to play in the ad hoc network. One major assistance of this scheme is that the nodes do not need to dissolutely eavesdrop to the traffic short-lived through their neighbors. The data about the malicious nodes is collected effectively by using experiments. This reduces the overhead on the network meaningfully. The FACES algorithm is divided into four stages, as encounter Your Neighbors, Rate Friends, Share Friends and Route finished Friends. The first three stages of the algorithm are broken, while the fourth is on demand. The algorithm offers authentication of nodes by sending an initial challenge. Nodes which have completed the charge find place in the friend list. A node which does not wide the testing is erased to the enquiry mark list, which is a list, holding data about the malevolent nodes. It signifies uncertainty on the node, and it is later not used in the directing process. The question mark list also supplies the nodes which destroy from the position of friend node by execution malicious activities. Friends are rated on the basis of the total of data they transfer finished themselves and according to the evaluation of other friends, which is acquired during the friend list allotment process. The rating is on a scale of zero to ten. When a node decides to conduct data, it shows a direction request message, as required by the cause routing algorithm. Each transitional node forwards route request message only if the transfer node is not in the question mark list. On delivery the route reply messages, the source node calculates the root by checking for friends in the route. The data is to conclude sent through the route with the greatest number of consistent friends. The quality of the route is determined by estimating each and every node in the route and making a ultimate conclusion about the value of the route.

2.3. Mitigating routing Misbehavior in MANET

Marti *et al* [3], proposed a mechanism called as watchdog and pathrater on DSR to identify the mischievous nodes in MANETs. The approach presents two extensions to DSR: A watchdog detects misbehaving nodes, by preserving a buffer of communicated packets and eavesdropping of other node forwarding's. It links each eavesdropped packet with the packets in the defense to see if there is a equal. If so, the packet in the buffer is removed and disremembered by the watchdog, since it has been advanced on. If a packet has remained in the buffer for longer than a definite timeout, the watchdog increases a failure count for the node blamable for forwarding on the packet. If the tally overdoes a certain onset bandwidth, it decides that the node is misbehaving and directs a message to the basis alerting it of the mischievous node. A pathrater evades routing packets through the detected malicious nodes. Each node evaluations a link metric with respect to the consistency of links and information about misbehaving nodes. A node assigns this metric to links to every other known node and sometimes informs the metric.

2.4. Lightweight Sybil Attack

This method is known as trivial as it does not use any extra hardware or aerials for its execution. It is used to detect Sybil Attacks. It includes three steps:1) Types of Sybil nodes: There are two types of Sybil nodes. In first type it concurrently use many personalities at a time either by spoofing others identities or by creating its own personalities. In second type it uses one personality at a time.2) Threshold value: In this authors supposed that usual nodes do not have quickness greater than 10mtr/s. The nodes whose speed is greater than 10m/s are detected as Sybil nodes.3) Comparison: In this RSSs (Received Signal Strength) upper bound threshold value is calculated. The upper bound value is calculated as average of RSSs value when nodes are moving at 10mtr/s speed. When new node enters in a network then its RSSs value is compared with RSSs upper bound value, if it is greater or equal to upper bound RSS value then it is detected as Sybil node.

3. Existing System

A node is detected to exhibit selfish behavior if it is not relaying the received packets even if it is active in the network. It may be due to factors such as:

- low energy
- low data rate
- poor channel conditions

This can be detected by analyzing the routing table of the neighbor nodes of the malicious node. If the routing table information of the neighbor does not get updated then selfish behaviour can be detected.

4. Proposed Work

This problem of isolating selfish nodes can be analyzed in two folds. First, the analysis is based on the available energy of the mobile nodes, which strongly predicts the possibility of a cooperative mobile node to change its behaviour into a selfish node. Secondly, reconfirmation of the nodes' selfishness can be estimated based on exponential reliability factor and decision on isolating them from the routing path is incorporated.

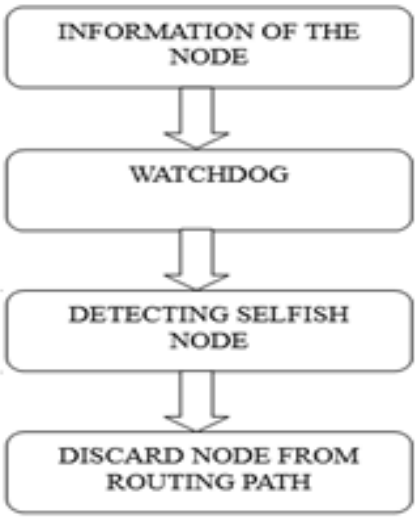

Fig 2

5. Methodology

5.1. Energy Based Selfish Node Detection

This Residual Energy parameter based Selfish Node Isolation Model computes the available energy metric (E_m) of the mobile nodes in the routing path between the source and destination node based on the residual energy (Re_m), which is defined as the amount of initial energy possessed by the mobile node before data transmission and the energy drain rate (Dr_m), which is defined as rate of energy dropped by the mobile node for participating in the routing activity. This available energy metric of the mobile node at any time instant's' is given in (1)

$$E_m = \frac{Re_m}{Dr_m} \quad (1)$$

Where, the drain rate of a mobile node is calculated using exponential weighted moving average method given through (2).

$$Dr_m = \alpha \times Dr_k + (1-\alpha)Dr_{k-1} \quad (2)$$

Here,Dr_k and Dr_{k-1} indicates the drain rate of a mobile node in two successive sessions and α is defined as the weighted average calculated through (3).

$$\alpha = \frac{2}{k} \quad (3)$$

Where 'k' indicates the number of sessions.

When the computed value of available energy metric E_m is found to be less than the threshold energy E_{th}which is important for a mobile node to be in supportive state, then the mobile node is identified as selfish. The value of threshold energy E_{th}proposed for our mathematical model is considered as 50Joules. When the mobile nodes present in the routing path established between the source and destination nodes are identified as selfish through available energy metric, the decision of isolating them can be incorporated through a factor called Moving average based reliability factor (MABRF). This Moving average based reliability factor (MABRF) for a mobile

$$dp = n - rp \quad (4)$$

The packets are sent to different nodes in a routing protocol, among those node the watchdog can be detected. And Isolate the selfish node from the different set of nodes and discard the egotistic node from routing path.

6. Evaluation Result

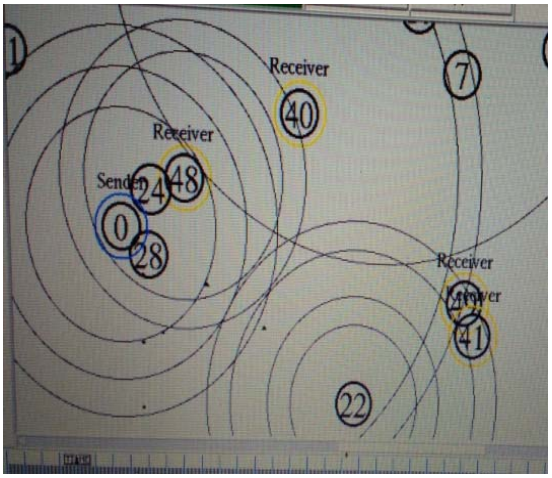

Fig 3: packet dropped

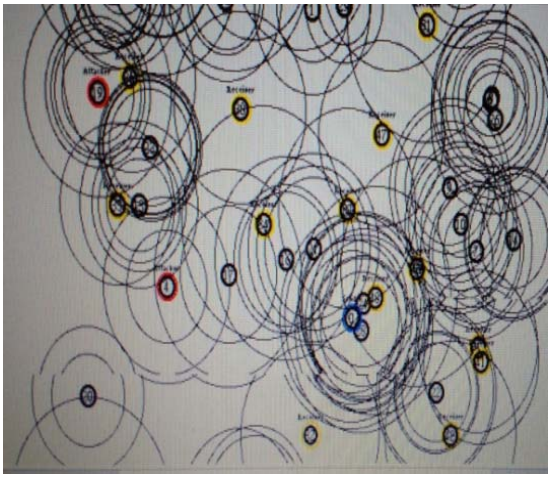

Fig 4: Attack Detected

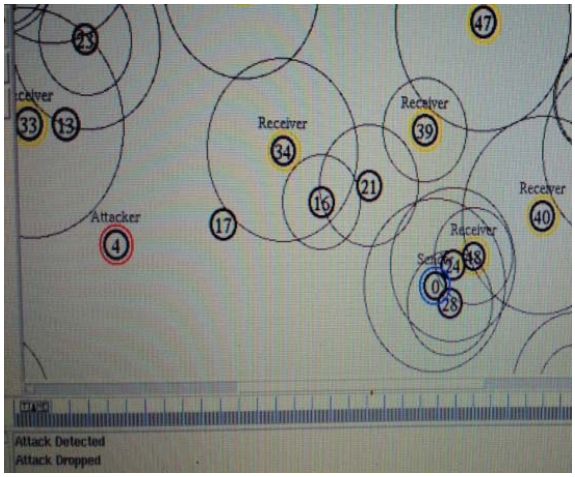

Fig 5: Attack dropped

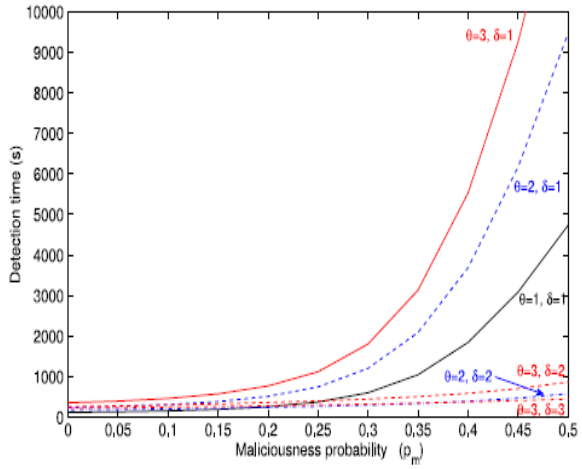

Fig 6: Graphical notation

Conclusion

This paper proposes as a cooperative contact -based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the injurious effect of wrong positives, false negatives and malicious nodes. If the reliability factor for a mobile node is found to be less than 0.4, then the node is reconfirmed as selfish and isolated from the routing path. This prediction of selfish nodes could enable the rehabilitation of the entire network so that the performance could be enhanced. This exponential reliability factor also enables the neighbor nodes for detecting selfish nodes in a reformist manner. As a part of the upcoming work, we are planning to devise a reputation based mitigation mechanisms that incorporate Cranach's statistical coefficient for identifying selfishness behavior of mobile nodes.

References

1. Amir Khusru Akhtar, Sahoo G. Mathematical model for the detection of selfish nodes in MANETs. Int J Comput Sci Inform. 2009; 1(3):25-8.
2. Bo Wang, Sohraab Soltani, Jonathan Shapiro K. Pang – Ning Tan. Local detection of selfish routing behaviour in ad hoc networks. In: Proc., 8th IEEE international conference on parallel architectures, algorithms and networks, 2005; 1(1):16-22.
3. Chen TM, Varatharajan V. Dempster–Shafer theory for intrusion detection in ad hoc networks. IEEE Internet Computing 2009; 3(1):234-41.
4. Pusphalatha M, Revathy V, Rama Rao P. Trust based energyaware reliable reactive protocol in mobile ad hoc networks. World Acad Sci, Eng Technol 2009; 3(27):335.
5. Marti S, Gulli TJ, Lai K, Baker M. Mitigating routing misbehaviour in mobile ad hoc networks Mobile Computing and Networking. In: Proc., 6th ACM Annual International Conference on Mobile Computing and Network (ACMMobiCom), Boston, USA, 2000; 1(1):255-65.
6. Michiardi P, Molva R. CORE: a collaborative reputation Mechanism to enforce node cooperation in mobile ad hocnetworks. In: Proc., 6th IFIP Conf. on Security, Communications and Multimedia, Protoroz, Solvenia, 2002; 228(1):107-21.
7. Buchegger S, Boudec JY. Performance Analysis of the CONFIDANT protocol: Cooperation of Nodes – Fairness inDistributed Ad-hoc Networks. In: Proc., 3rd ACM International Symposium on Mobile ad hoc Networking and Computing (MobiHoc '02), New York, USA, 2002, 1(1).