ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Identification Technique for All Passive Selfish Node Attacks In a Mobile Network

Sumiti[1]
MMICT & BM (MCA) Department
MM University
Mullana (Ambala) - India

Sumit Mittal[2]
MMICT & BM (MCA) Department
MM University
Mullana (Ambala) – India

Abstract: ***The focus of this work is on detection of passive path selfish node in mobile network. Earlier techniques for detection were based on statistical or signature. These techniques were useful for identifying the selfish nodes in active path only. But in this work, distributed agent based technique is proposed for identifying passive path selfish nodes. Agents based technique is designed for gathering the information from various nodes. Every node is like a monitoring module and its task is to check the neighbouring nodes, to observe their behaviour and then to check out whether the node is selfish or not. Each node sends the message related to its first hop neighbour node and they evaluate node based feedback from neighbour nodes. Agent runs an observation technique to get the conduct data from its neighbouring nodes. The proposed technique is able to isolate Selfish Nodes easily and increases the security of network at a minor cost of overhead in coordinating nodes.***

Keywords: MANET, Selfish Node Attack, Identification Technique, Distributed Agent Based Approach.

I. INTRODUCTION

With the rapid development in wireless technology, ad hoc networks have emerged in many forms. Mobile ad hoc network operates in the license free frequency band and do not require any investment in infrastructure, making them attractive for military and commercial applications. Now a days, securing the network being one of the major concerns. Ad hoc networks are vulnerable to attacks due to many reasons. Amongst them are lacks of secure boundaries, threats from compromised nodes inside the network, lack of centralized management facility, restricted power supply, scalability etc. MANETs are mostly off guarded. Hence malicious node changes its code and getting personal data like cryptographic keys is easily possible for a malicious node. Mobile network is broadcast in open environment. So there are different attacks and these attacks can interrupt the operation of MANETS. In this paper, we have focused on passive selfish node attack. In this attack, when the nodes receive the data and do not send to next node are known as selfish node. These nodes want to save their resources such as energy source. Such nodes disturb the operation of the network and waste the resources of regular nodes. So here is the focus to find out selfish node and isolate it in the network.

a) Attacks

Any secure networking system must provide the following six properties: Secrecy, authenticity, integrity, availability, non-repudiation and access control. But due to the open medium communication; there are many types of attacks on MANETs such as Denial of Service attack, Information theft attack, Intrusion and Tampering and selfish node attacks that disturb the security goals. In this paper focus is on detect selfish nodes from passive path.

II. SELFISH NODE ATTACK

Selfish node wants to save its resources to the maximum. Selfish node rejects all incoming packets (control and data) except those which are destined to it. Nodes would not be included in the routing by falling control packets and then be released from being requested to forward data packets. Similarity of both types of misbehaving is that they operate the network to send

their own packets but say no to give the same services back. Misbehaving nodes significantly degrade the operation of a MANET. These nodes use the network and its services for their own use and they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves. These nodes do not take participation in network activities, by which network performance degrade sharply.

III. Related Work

The Misbehaviour problems including MANETs have been studied by many researchers. In MANETs, various techniques have been proposed to prevent selfishness.

Marti et al. [8] proposed a *watchdog* and *pathrater* scheme. *Watchdog* keeps track of misbehaving nodes. *Pathrater* avoids routing through those misbehaving nodes.

Buchegger and Le Boudec et al. [2] proposed the *CONFIDANT* protocol. *CONFIDANT* consists of four important components-Monitor, Reputation System, Trust Manager and Path Manager, which perform all function collectively to rate the node and then generate alarm if node is malicious.

K. Balakrishnan et al. [13] proposed the 2ACK scheme that does not rely on end-to-end acknowledgment. Such an acknowledgment scheme does not exist in some traffic flows (such as UDP). Instead, the 2ACK scheme tries to detect misbehaving links as the links are being used. This combined scheme, the 2ACK transmission and the monitoring processes are turned on only when routing performance degrades. It further reduces the routing overhead of the 2ACK scheme.

Kejun Liu et al. [14] proposed the 2ACK scheme to mitigate the adverse effects of misbehaving nodes. The basic idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the destination node sends back a special two-hop acknowledgment called 2ACK. It indicates that the data packet has been successfully received. Such a 2ACK transmission takes place for only a fraction of data packets, but not all. Such a "selective" acknowledgment is intended to reduce the additional routing overhead caused by the 2ACK scheme. Judgment on node behaviour is made after observing its behaviour for a certain period of time.

IV. Detection Techniques

Several systems have been proposed for find out the misbehaving nodes in MANETs, which are classified into three categories:

a) Credit Based System

Credit-based system is designed for forward the packets in the form of virtual money (specifically called as Credit). In this system, nodes earn Credit by providing forward services to others nodes and have to pay to get services from other nodes [1]. However, for protect of the Credit value from attacks and modification; some costly security modules independent of nodes are to be used. A well-behaved node that is not asked about route enough packets could not earn credits and that is unable to send its own packet [2]. The fundamental thought of credit-based system is to motivate the nodes for reliably perform functions of the network. When they demand different node, they help them in message sending and utilize same payment scheme [15].

b) Reputation Based System

A reputation-based system, according to each node behavioural pattern, builds a reputation metric. In this monitoring is called a watchdog [1]. The reputation of a neighbour is evaluated using only locally available information. It is reported by direct observations of the neighbour. It performs almost better comparison schemes that share second-hand reputation information [3] [5].

c) Acknowledgement Based System

In this the receiver of acknowledgment verifies that a packet has been forwarded. Liu et al. [14] propose the 2ACK system where nodes send acknowledgment for verify cooperation. Because colluding nodes can claim that not receive the acknowledgment. All of the mechanisms are designed for detect and handle misleading nodes. There are few systems that have been proposed for detect selfish nodes in a MANET. Huang et al. [18] suggest the monitoring node compares the ratio of relay RREQ number between its neighbour node and itself. If the ratio is smaller than a threshold, the neighbour node is regarded as selfish node and its packet is dropped as the punishment.

V. PROPOSED DISTRIBUTED AGENT BASED APPROACH

In this technique, two agents (Global agents) are designed. These agents are designed for gathering the information from various nodes. In this technique, data is gathered from various nodes in two phases. In the first step, every node is like a watch module and its task is to check the neighbouring nodes and to observe their behaviour and check out for the node whether it's selfish or not. Each node sends the message to its adjacent first hop neighbours node.

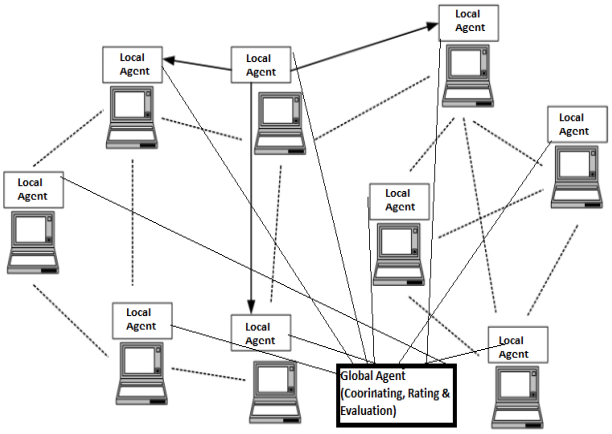

Fig. 1 Coordination between all Local agent and Global agent

According to figure 1, every node in the mobile ad hoc network participates in the detection activities. Neighboring nodes share their investigation results with each other and cooperate in a broader range. After that the agent runs an observation technique to get the conduct data from the neighbouring nodes. The system encourages the cooperating nodes for providing quick service. As in the figure 2, Yellow link shows – link between agents and nodes, Green link shows – secure link between two agents and Red Link shows – this node is selfish node. Agent builds a table for selfish and normal operating node. Agent uses coordination, cooperation, rating mechanism and evaluating mechanism for finding out the node whether it's selfish or not.

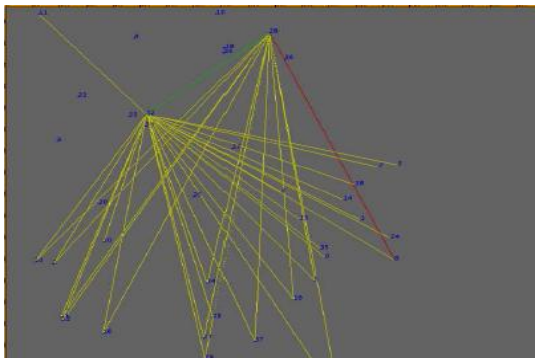

Fig. 2 Distributive Agents based approach

VI. ALGORITHM FOR RATING AND EVALUATING OF SELFISH NODE

Algorithm for Selfish Node (Rating and Evaluation)

Set mobile node = M //Total Mobile Nodes

Set source node = S //S Є M

Set Destination Node = D // D Є M

Start simulation time = t0

Set radio range = rr; //initialize radio range

Set Local agent = p; // local agent

» ***Evaluating Mechanism***

SRs ← secondary rating of the node under analysis, S

PRs ← primary rating of the node under analysis, S

if mechanism for detection of false HELLO or false TC generation has identified S as selfish or misbehaving node then

PRS ← PV

else

if SRS < PRS then

SRS ← SRS + SRV

else

PRS← PRs + PRV

end if

end if

if (SRS < 0.5) and (PRS<0.5) then

Node is Selfish

else

Node is cooperative

end if

» ***Rating Mechanism***

Check_Selfishness (S,D,M)

{

If ((nodeЄ M) && (pkt< 100 pkts/ms)

{

pkt accepted by neighbor;

pkt_Accept_limit();

}

Else { Node_Selfish()

{ can't accept by neighbor ;

Block pktssender ;

}}}

Node out of range;

}

a) Rating Mechanism

Every node is like a watch module and its task is to check the neighbouring nodes and to observe their behaviours. Firstly check all hop neighbours by each node and then count all messages that are received and sent by the nodes. Information is saved and then is sent for evaluating mechanism. In a specific time period saved information is updated.

b) Evaluating Mechanism

This mechanism utilizes the extent of the amount of messages, the message transmitted by a node and messages received or gained by a node from cooperative nodes. This evaluating mechanism is the degree to decide that node is malicious or cooperative; this is based on the amounts of send packets and amount of gain packets. Agent is maintaining a table for evaluating each node and monitors all its one hop neighbours. The range of the value evaluation factor 'E' is between 0 and 1. If the value of that node in its evaluation table is near to 0 than these nodes are consider as selfish nodes, if the value is near to 1; then these nodes are known as cooperative nodes.

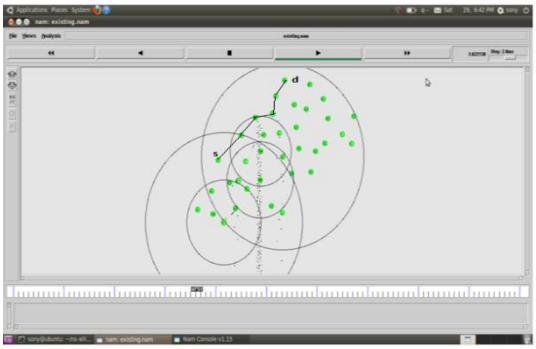

Fig. 3 Shows the passive path

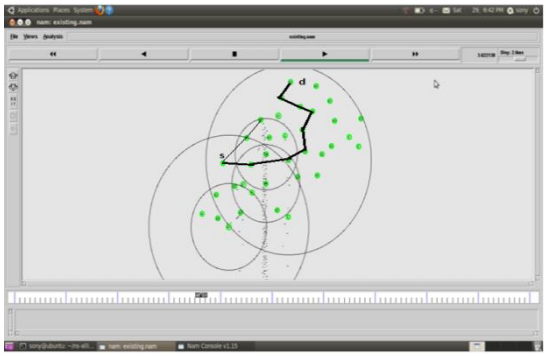

Fig. 4 Shows the passive selfish node

In figure 3, a node in the path act as selfish node, this drops the packets. After detecting this selfish node; the path is changed and a new path is followed, this new path is longer than previous path, so some overhead is increased in detecting and coordinating new path between nodes. The proposed technique is able to isolate the selfish node in an efficient manner. The security of network increases at a minor cost of overhead.

VII. COMPARISON

In this section, proposed distributed agent based technique is compared with existing techniques and then we find out that this proposed technique is better than existing technique

TABLE 1

Comparison of Selfish Node Attack Detection Techniques

Techniques	Merits	Demerits
TrustModelling based	Trustworthiness of nodes are considered Secure Routing	Traffic overhead due to TRR
Reputation Management based	Behaviour of nodes are analysed	Approach only based on selfish nodes
Anomaly based IDS	Anomalies events are diagnose both in accidental errors and intentional attacks	Selfish nodes refuse to run IDS
Wathdog and pathrater	Increase throughput	Transmission overhead
Risk awareness to MANET routing attack	Reduce network partitioning due to isolation of malicious nodes	Packet overhead and bye overhead
Proposed Distributed Agent based Approach	Selfish Nodes are easily isolated. Behaviour of nodes is analysed in easy and better manner. Efficiency & security increases.	Overhead increases because of coordination between nodes.

VIII. CONCLUSION

A mechanism for detecting selfish nodes is proposed, this mechanism is focused on detecting passive communication path in the network. Selfish nodes in the network do not provide any services and reserve resources for network operations. The proposed technique detects selfish nodes, which don't forward Route Request packets; and different number of selfish nodes in the network performing different action. We are able to detect selfish nodes at a higher rate of detection, when the numbers of selfish nodes are more, but on a few selfish nodes are detected at lesser detection rate. In this paper, we compared the proposed distributed agent based technique with existing techniques and find out that the proposed technique is better than other existing techniques. Here we have focused on the selfish nodes, but this work can be extended to detect other type or behaviour of selfish nodes which can help in improving performance of MANET.

References

1. Wu, Lien-Wen and Rui-Feng Yu, "A threshold-based method for selfish nodes detection in MANET", IEEE International Computer Symposium (ICS), 2010.
2. S. Buchegger and J.Y. L. Boudec, “Performance analysis of the Confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)”, MOBIHOC'02, 2002.
3. J. Mundinger and J.Y. L. Boudec, “Analysis of a reputation system for mobile ad-hoc networks with liars”, Journal on WIOPT, 2005.
4. Bakar, KhairulAzmi Abu, and James Irvine, "A Scheme for Detecting Selfish Nodes in MANETs using OMNET++", 6th IEEE International Conference on Wireless and Mobile Communications (ICWMC), 2010.
5. Safaei, Zahra, Masoud Sabaei and Fatemeh Torgheh, "An efficient reputation-based Mechanism to enforce cooperation in MANETs," IEEE International Conference Application of Information and Communication Technologies, (AICT) 2009.
6. Yogesh Chaba, Yudhvir Singh, Preeti and Deepak, “Performance analysis of various Distributed denial of service based attacks in mobile ad hoc networks”, IEEE International Conference Advance Computing Conference (IACC) March 6-7, 2009, pp 3228-3132.
7. Samreen, Shirina and G. Narasimha, "An efficient approach for the detection of node Misbehaviour in a MANET based on link misbehaviour", 3rd IEEE International Advance Computing Conference (IACC) 2013.
8. S. Marti, T. Giuli, K. Lai and M. Baker, “Mitigating routing misbehavior in mobile ad hoc Networks”, in the 6th ACM International Conference on Mobile Computing and Networking, 2000.
9. Prabha Rani, Yogesh Chaba and Yudhvir Singh, “Hybrid Approach for Detection and Prevention of Blackhole Attack in Mobile Ad hoc Network”, International Journal of Wireless Communication, ISSN: 0974-9640, August 2011, pp 885-890.
10. Yogesh Chaba, Yudhvir Singh and Preeti, “Detection of Malicious Packet Dropping Based DDOS Attack in MANET”, Journal of Computer Science, ISSN: 0973-2926, Vol. 3, Issue 2, pp 959-964, Jan-Feb 2009.
11. Hernandez Orallo, Enrique et al. "Improving selfish node detection in MANETs using a Collaborative Watchdog", IEEE Communications Letters, volume 16, issue 5, pp 642-645, 2012.
12. Yudhvir Singh, Yogesh Chaba, “Detection and Prevention of Blackhole Attack in Mobile Ad hoc Network”, IEEE International Conference on Advance Computing Conference (IACC), pp 2668-2672, March 6-7, 2009.
13. Balakrishnan, Kashyap, Jing Deng and Pramod K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks", IEEE Transaction on Wireless Communications and Networking Conference, Volume 4, 2005.
14. Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs", IEEE Transactions on Mobile Computing, volume 6, issue 5, pp 536-550, 2007.
15. Koshti, Dipali and Supriya Kamoji, "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, 2011.
16. Yogesh Chaba, Yudhvir Singh and Preeti, “Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET”, Journal of Networks, Academy Publisher, ISSN : 1796-2056.
17. Roy, Debdutta Barman and Rituparna Chaki, "Detection of Denial of Service Attack Due to Selfish Node in MANET by Mobile Agent", Recent Trends in Wireless and Mobile Networks, Springer Berlin Heidelberg, pp 14-23, 2011.
18. Buchegger, Sonja and Jean-Yves Le Boudec, "Performance analysis of the CONFIDANT Protocol", Proceedings of the 3rd ACM international Symposium on Mobile ad hoc networking and Computing, 2002.
19. Vijayan, R., V. Mareeswari and K. Ramakrishna, "Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic", International Journal of Research and Reviews in Computer Science, volume 2, issue 3, 2011.
20. Wang, Yongwei, Venkata C. Giruka and Mukesh Singhal, "A Fair Distributed Solution for Selfish Nodes Problem in Wireless Ad hoc Networks", Springer Berlin Heidelberg, pp 211- 224, 2004.
21. Sumiti, Sumit Mittal, “Characterization of Routing Approaches in Mobile Network: A Study”, IJARCSSE, ISSN: 2277 - 128X, Volume 4, Issue 10, pp 108-111, October 2014.
22. Sumiti, Sumit Mittal, “Detecting Selfish Node over the Active Path using Neighbor Analysis based Technique”, International Journal of Science and Research, ISSN: 2319-7064, Volume 4, Issue 3, pp 1295-1298, March 2015

