ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Survey on the Selfish Node Detection in the Mobile Ad-Hoc Network

Priyanka Deokar[1], Dipalee Gothwal[2]

M.E. Student, Dept. of Computer, D.Y.Patil College of Engineering, Akurdi Pune, India[1]

Assistant Professor, Dept. of Computer, D.Y.Patil College of Engineering, Akurdi Pune, India [2]

ABSTRACT: Mobile ad-hoc networks (MANETs) is receiving significant attention in the wireless mobile networking field. In MANET nodes communicate with each other on the basis of unique identity that forms the one to one mapping between an identity and an entity and that is usually assumed either implicitly or explicitly by many protocol mechanisms; hence two identities represents two different nodes. But the malicious nodes can illegitimately claim multiple identities and violate this one-to-one mapping of identity and entity philosophy and this type of malicious attack is called Sybil attack. The MANET network also faces other problem like the presence of selfish node. A selfish node will typically not cooperate in the transmission of packets, seriously affecting network performance. Although less frequent, nodes may also fail to cooperate either intentionally (a malicious behaviour) or due to faulty software or hardware.

KEYWORDS: Watchdog, MANET, Selfish node.

I. INTRODUCTION

MANET is a widely used network with plenty of users frequently changing. The users in this type of network need security and surety of their data getting transferred without fail. Many measures should also be taken to make sure that the data transferred by the users does not get lost in the MANET.

There are various reasons of data getting lost in MANET. One reason from many is presence of selfish node and malicious nodes. The presence of these two nodes can create major problems like network failure. Therefore , measures are taken to prevent these type of nodes.

A. *SELFISH NODE:*

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.

B. *MALICIOUS NODE:*

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 .

DOI: 10.15680/IJIRCCE.2017. 0501153

II. RELATED WORK

There are several detection techniques for detetcting the selfish nodes. All these techniques are classified into three categories :

1. Credit Based System
2. Reputation Based System
3. Acknowledgement Based System

A. A COLLABORATIVE CONTACT-BASED WATCHDOG :

Collaborative Contact based Watchdog as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network. The goal of this approach is to reduce detection time and to improve the precision by reducing the effect of both false negatives and false positives.

B. RECORD- AND TRUST-BASED DETECTION :

The main goal of this analysis is to handle and detect selfish nodes in MANET using the Record and Trust Based Detection technique(RTBD).

Here the behaviour of the node decides the trustworthiness of the node. RTBD method significantly increases the detection ratio. Detection of the selfish nodes is done in an efficient manner. The suggested RTBD method is an effective method, which enhances the performance of MANET.

Selfish node detection is based on data packet drop. Then, the selfish node is checked for false reporting; when the node misreports the data, it is block listed. These processes repeat for all the mobile nodes in MANET, thus obtaining the set of selfish nodes from the selfish nodes in the network. The packet transmission and the block list will decide whether the packet is available or not. All the aforementioned processes are repeated for the transfer of all packets. The packets are transmitted one by one at each iteration step until there is no packet available for further transmission. Each trust node receives the trust reports for each data packet transfer. The records are signed for further authentication and protection.

C. A MUTUAL REINFORCEMENT MODEL FOR TRUSTWORTHY ONLINE RATING SYSTEMS

The average of customer ratings on a product, which is called a reputation, is one of the key factors in online purchasing decisions. There is, however, no guarantee of the trustworthiness of a reputation since it can be manipulated rather easily. The paper defines false reputation as the problem of a reputation being manipulated by unfair ratings and design a general framework that provides trustworthy reputations. For this purpose, author has proposed TRUE-REPUTATION, an algorithm that iteratively adjusts a reputation based on the confidence of customer ratings.The effectiveness of TRUE-REPUTATION through extensive experiments in comparisons to state-of-the-art approaches.

The above mentioned techniques are all proposed for detection of selfish node. But still the techniques are different from each other like follows: [1].

Parameters	*CoCoWa*	*RTBD*	*True -Reputation*
Detection of selfish node	*Yes*	*Yes*	*Yes*
Re-routing of packets	*No*	*no*	*No*

Table 2.1 Comparison of techniques

The table 2.1 shows the different approaches how they differ from each other.

III. SIMULATION RESULTS

The simulation studies involve the deterministic small network topology with 5 nodes as shown in Fig.1. The proposed energy efficient algorithm is implemented with MATLAB. We transmitted same size of data packets through source node 1 to destination node 5. Proposed algorithm is compared between two metrics Total Transmission Energy and Maximum Number of Hops on the basis of total number of packets transmitted, network lifetime and energy consumed by each node. We considered the simulation time as a network lifetime and network lifetime is a time when no route is available to transmit the packet. Simulation time is calculated through the CPUTIME function of MATLAB. Our results shows that the metric total transmission energy performs better than the maximum number of hops in terms of network lifetime, energy consumption and total number of packets transmitted through the network.

The network showed in Fig. 1 is able to transmit 22 packets if total transmission energy metric is used and 17 packets if used maximum number of hops metric. And the network lifetime is also more for total transmission energy. It clearly shows in Fig. 2 that the metric total transmission energy consumes less energy than maximum number of hops. As the network is MANET means nodes are mobile and they change their locations. After nodes have changed their location the new topology is shown in Fig .3 and energy consumption of each node is shown in Fig. 4. Our results shows that the metric total transmission energy performs better than the maximum number of hops in terms of network lifetime, energy consumption and total number of packets transmitted through the network.

IV. CONCLUSION AND FUTURE WORK

Selfish node is a serious problem in the MANET that needs to be detected as soon as possible. Various techniques are proposed but don't work over re-routing of the lost packets. Hence re-routing of the lost packets can be combined with one of the techniques to assure more reliability of the network.

REFERENCES

1. Enrique HernandezOrallo, Manuel David Serrat Olmos, Juan Carlos Cano,Carlos T. Calafate, and Pietro Manzoni, "CoCoWa: A Collaborative Contact Based Watchdog for Detecting Selfish Nodes," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.14, NO. 6, JUNE 2015.
2. Wenjia Li and Houbing Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," IEEE RANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 17, NO. 4, APRIL 2016.
3. Jebakumar Mohan Singh Pappaji Josh Kumar,Ayyaswamy Kathirvel,Namaskaram Kirubakaran,Perumal Sivaraman and Muthusamy Subramaniam, "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT," Springer 23 May 2015.
4. T.R. Srinivasan and K.G. Chithra, "Detection and Isolation of the Selfish Nodes Using a Collaborative Contact Based Watchdogs," Middle-East Journal of Scientific Research 24,IDOSI Publications, 2016.
5. Hyun Kyo Oh, Sang-Wook Kim, Sunju Park, and Ming Zhou , "Can You Trust Online Ratings? A Mutual Reinforcement Model for Trustworthy Online Rating Systems," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 45, NO. 12, DECEMBER 2015.
6. Sumit Mittal, Department MM University Mullana (Ambala) , "Identification Technique for All Passive SelfishNode Attacks In a Mobile Network," International Journal of Advance Research in Computer Science and Management Studies,Volume 3, Issue 4, April 2015.
7. Anamika Pareek and Mayank Sharma, "ARCHITECTURE FOR DETECTION OF SYBIL ATTACK IN MANET USING MAC ADDRESS," International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: Issue 6, Volume 2 (June 2015).
8. Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, "Lightweight Sybil Attack Detection in MANETs," IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013.
9. Enrique Hernandez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, "Improving SelfishNode detection in MANETs Using a Collaborative Watchdog," IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 5, MAY 2012.
10. C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs, "Int. J. Wireless Mobile Netw., vol. 3, no. 2, pp. 2937, Apr. 2011.
11. M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks," IEEE Trans. Mobile Comput., vol. 10, no.7, pp. 9971010, Jul. 2011.
12. A. Passarella, and M. Conti, "Characterising aggregate intercontact times in heterogeneous opportunistic networks," in Proc. 10th Int. IFIP TC 6 Conf. Netw., 2011, pp. 301313.

BIOGRAPHY

Priyanka Deokar is a Associate at 3DPLM Global Services and also persuing Master of Engineering (M.E) in Computer Science from D.Y.Patil College of Engineering Pune.

DOI: 10.15680/IJIRCCE.2017. 0501153