International Journal of Engineering & Technology, 7 (4.39) (2018) 206-209

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Approach for Detection of Selfish Nodes in MANET

Ishu Varshney[1], Shahjahan Ali[2], Bhairvee Singh[3]

Assistant Professor, Department of Computer Science & Engineering, GLBITM, Greater Noida, Uttar Pradesh, INDIA
Assistant Professor, Department of Computer Science & Engineering, SRMSCET, Bareilly, Uttar Pradesh, INDIA
**Corresponding author E-mail: varshneyishu25@gmail.com*

Abstract

MANET (Mobile Ad-hoc Network) is self-arranging framework using more than one mobile wireless node. The misbehaving of nodes is due to the selfish motives that appreciably decline the performance of MANET. So, it's essential to detect the selfish nodes to improve the overall potential of transmitting the data packet. Therefore, this paper basically deals with an approach on detection of selfish nodes in MANETs that further simulated in NS-2.

Keywords: *MANET; mobile wireless nodes; Selfish nodes; data packet;*

1. Introduction

MANET is a huge research field within the wireless community due to its vast applications. MANET is a temporary connection between the computers and the devices for the sharing of information in the form of a data packet. So in figure 1, firstly the path for transmitting the data packet information from sender S to receiver D is S-A-D. MANET [1] is free to move separately as having an ability of changing its link randomly from one device to another frequently. So due to mobility, the path has been changed from Source S to intermediate nodes B, C, A and at last to the destination D as shown in figure 1. It's a multi-hop fashion as each device in this network topology acts as a router.

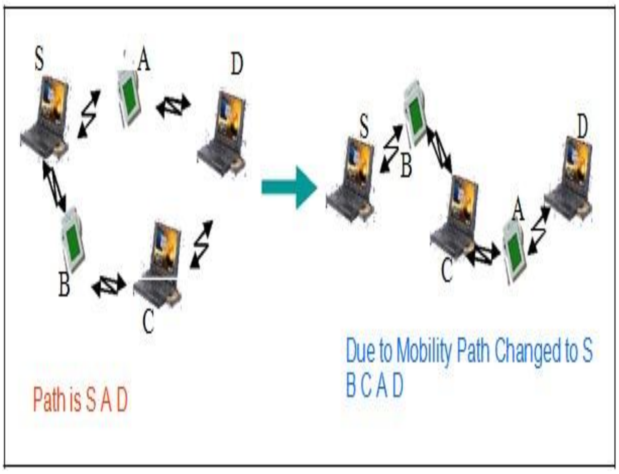

Fig. 1: Scenario of MANET

The topology that formed is dynamic in nature that it means that topology changes with time, therefore, the problem of routing occurs. Due to this while transmitting data packet information from source to destination is done through intermediate nodes that may act as a misbehaving node or selfish node. [2].

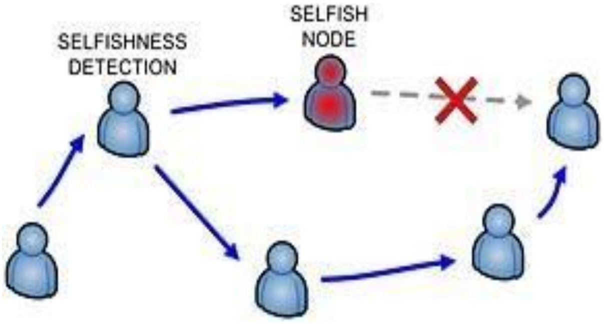

Fig. 2: Effect of Selfish node [2]

For transmitting the packet from one hop to the next uses a concept of RREQ message and RREP message. When one node transmits a message to neighbor's node, it means RREQ message send i.e. route request and when destination reply to the node from where it gets the request means route reply. Sometimes, RREQ messages immediately transmits the fake RREP to the sender then the selfish node drop the packet instead of forwarding as selfish node do not participate in routing shown in figure 3. This will affect the availability, dependability of the network topology. [2]

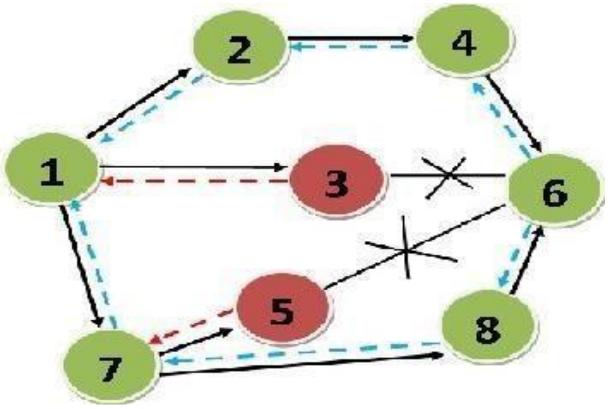

Fig. 3: Scenario of packet drop [2]

Paper is framed as: Section II gives the related background of detecting selfish nodes in MANET through various existing techniques; Section III discussed the proposed approach of my research work and Section IV conclusion and the future scope and paper end with References.

2. Related Background

In paper [3] proposed a watchdog and pathrater technique to improve the throughput of the network within selfish node behaviour that execute on the DSR protocol.
In paper [4] proposed scheme is to analyse the limitation in every three consecutive nodes in the path within the network are required to impart every transmitted data packet.
In paper [5] author proposed a scheme for resolving the issue of identifying misbehaving and forged acknowledgment data packets.
In paper [6] proposed the protocol to identify the selfish nodes using digital signature that helps in approving and verifying the acknowledgment packets.
In paper [7] proposed examination scheme to break down the data packet loss motives in WSN that extremely successful for static topology.
In paper [8] proposed the protocol to identify and respond the selfish nodes that it experiences the issue of clashing update reports that can't make correct decisions about node reliability.
In paper [9] proposed an scheme to ignore false attacking with the network.
In paper [10] proposed scheme to maintain the strategic distance from the attack examined discussed in paper 9 which filters the second-hand data.
In paper [11] proposed scheme that required to observing nodes to catch the activity in their transmission ranges and contended that such activity catching can prompt the fruitful identification of data packet dropping such as misrouting attacks can't be distinguished.
In paper [12] proposed CORE to assess the reputation of a node that keep up at every node to grab the different nodes reputation to decide if it is acting selfishly or not.
In paper [13] proposed a mechanism for MANET and WSN based on FGA technique that concentrate on ensuring the frameworks against various attacks. All the methodologies examined in this area is particularly under high node's mobility.

3. Proposed Approach

3.1. Architecture

There are basically five modules in the proposed system i.e. Data Collection Module, Data Processing Module, Node Characterization Module, Routing Performance Module and QoS Performance Module as shown in figure 4 consider these modules were present in each and every node required for transmitting the data packet information.

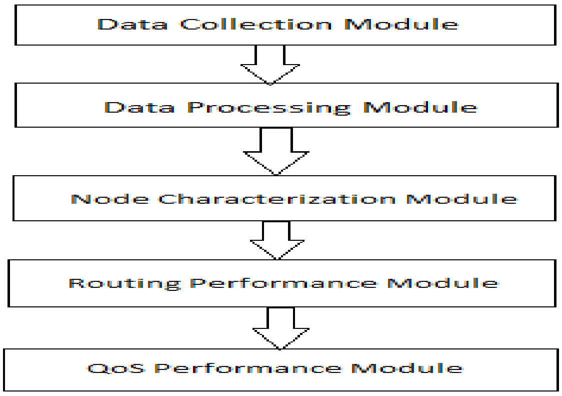

Fig. 4: Architecture of the Proposed Approach

3.2. Data Collection Module

Every node sends its monitored information Label_2 to all its neighbors and receives the same from its neighbors observed by them. This received information is kept in a different table Label_1.

$$Label\_1\,[i] \;=\; \frac{\sum_{j=1}^{Q} Label\_1_j[i]}{R}$$

$\forall \quad Label\_1_j[i] \neq 0 \;\&\&\; i \neq j$

where,

$Label\_1_j$ = Information shared by Node j

Q = Neighbor Nodes

R = $\sum_{j=1} 1 \;\forall$ Label_$1_j[i] \neq 0$ && $i \neq j$

N = Total Nodes in the network

i = Nodes in the network

3.3. Data Processing Module

Observing Technique: WATCHDOG S. Marti et al. [3] proposed the WATCHDOG approach for observing misbehaving nodes in the distributed topology shown and described in figure 5.

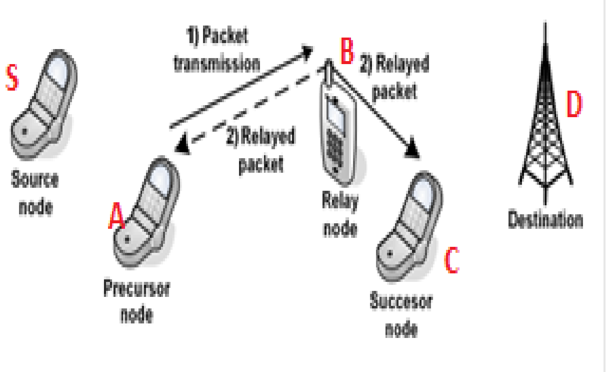

Fig. 5: Watchdog Detection Technique

Below is the example showing the four steps that define the working of watchdog technique:

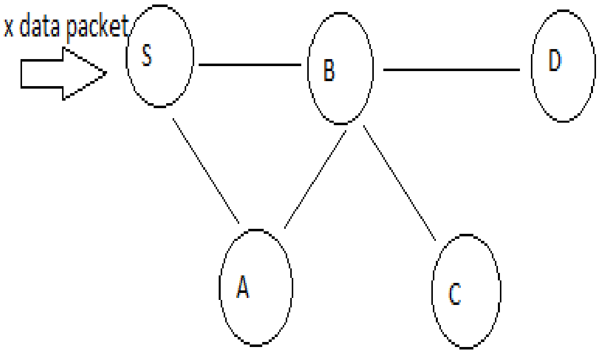

Fig. 6[Step1]: Node S having data x

Packet	Next Hop	Sending Time
x	B	T1

This above list is maintained by source node S and it contains the entry for every sent data packet.

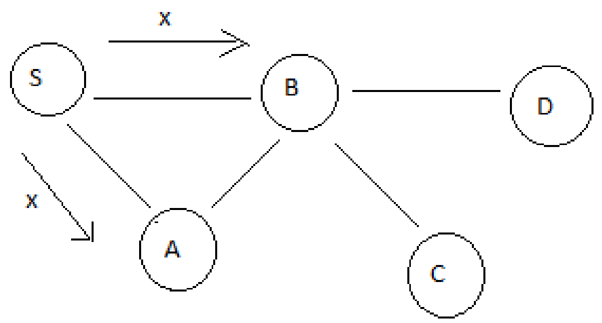

Fig. 7[Step 2]: Sender node S sends the packet

In above-mentioned figure 7, sender node S transmits the packet information to next node B to transmit to the next hop and keeps an entry for this data packet x in its buffer.

Packet	Next Hop	Sending Time
---	---	---

In above list, the entry is removed due to the overhead of the same data packet.

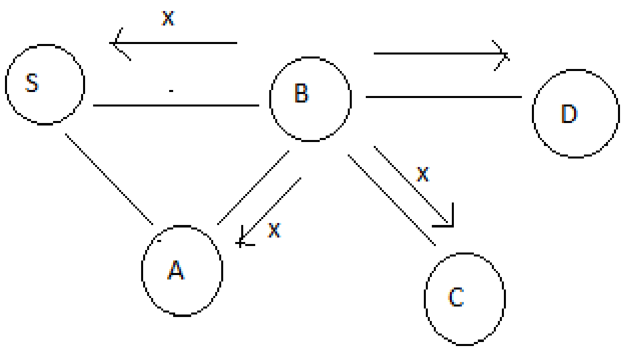

Fig. 8[Step 3]: Node B forwards data (Positive Behavior) Label_1A[B]—

If node B doesn't misbehave, it broadcasts the data packet information to its neighbor node. Node A overhears this and if this is within the timeout interval, the entry is removed from the buffer shown in figure 9. Node A now changes node B's behavior information accordingly.

Packet	Next Hop	Sending Time
X	B	T1

So the entry at the time of Step 2 now remains same in the list as shown above as it has not been overhead.

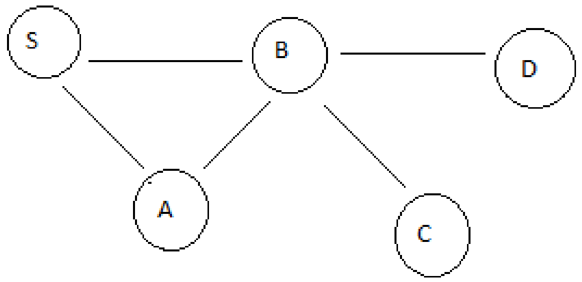

Fig. 9[Step 4]: Node B drops packet and that is detected by node A (Negative Behavior) Label_2A[B]++

However, if node B misbehaves, it does not broadcast the data packet information to its neighbors. Hence, node A does not overhear it. The entry for that data information remains for fixed time at node S. Therefore, node S increases the failures tally for that node responsible for transmitting the data information.

Threshold value and timeout interval that are used in deciding behavior of a node, are not predefined; they depend on various network conditions like congestion, bandwidth, and traffic etc. We choose an optimal value based on different experiments for threshold and timeout.

3.4. Data Processing Module

Here in this module all the gathered information is processed and finally stored in a table *Label_3* used for routing decisions.

$$Label\_3_{new}[i] = \frac{Label\_3_{previous}[i] + Label\_1\ [i] + Label\_2\ [i]}{f}$$

Where,

f referred as a variable whose value depends on Label_1 and Label_2 values as follows:

$f = 3$

$Label\_1\ [i] \neq 0\ \&\&\ Label\_2\ [i] \neq 0$

$f = 2$

$Label\_1\ [i] = 0\ \&\&\ Label\_2\ [i] \neq 0$

or $Label\_1\ [i] \neq 0\ \&\&\ Label\_2\ [i] = 0$

$f = 1$

$Label\_1\ [i] = 0\ \&\&\ Label\_2\ [i] = 0$

where,

N = Total no. of Nodes in the network

i ∈ Nodes in the network

3.5. Node Characterization Module

This module basically used to detect the selfish nodes and the packet dropped maliciously. Here, we avoid the selfish node from the routes from where the information has been collected, processed and observed.

Let some parameters that are used to detect the probability of packet dropped maliciously.

$P_{selfish}$ -- The probability that data packet is dropped maliciously.

$P_{congestion}$ -- The probability that a data packet is dropped due to the congestion in the network.

$P_{collision}$ -- The probability that data packet overhead due to the collision at sender's end.

$P_{timeout}$ -- The probability that a packet is forwarded after timeout time.

Then the probability that the packet is dropped maliciously is defined as:

$$P_{selfish} = 1\text{-}(P_{congestion} + P_{collision} + P_{timeout})$$

3.6. Routing Performance Module

This module describes how Routing Performance operates to help you understand that how to implement the technology in our network. After configuration, the Routing Performance technology runs through a series of phases that start with profiling data transmission, measuring the data transmission, apply policies for the transmission of data, controlling the data transmitting rate to meet the policy conditions, and finally verifying the result of the traffic class optimization.

3.7. QoS Performance Module

QoS (Quality of Service) particularly necessary for the transmission of the data packet with required parameters that quantitatively measure the QoS in terms of packet loss, bit rate, throughput, transmission delay, jitter control etc.

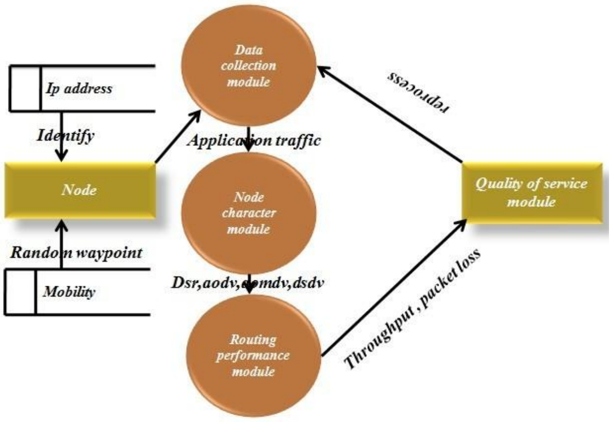

Fig. 10: Criterion for Performance of the Network

4. Conclusion

MANET is endangered to several attack because of its wide distribution of mobile wireless nodes. Here, we have discussed the issue of selfish nodes in MANETs as they sway the availability, efficiency, dependability, and reliability within the network. However, we proposed a theoretical approach for the detection of selfish nodes.

For future reference, examine the issue of data packet information on various nodes mobility. At the time of submission of this paper, we are under the process of creating a model for the above proposed approach in NS-2 Simulator.

References

[1] K. Azmi, A. Bakar and J. Irvine, “A Scheme for Detecting Selfish Nodes in MANETs using OMNET++”, in 6th ICWMC, 2010.

[2] J. Kaur, P. Singh, “Designing a Distributed Framework to Detect a Selfish Node in MANET by using a Collaborative Approach”, IJCST, Volume 4, Issue 4, August 2016.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in MANET”, in 6th Annual ICMCN, August 2000.

[4] Kejan Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs”, IEEE Transactions on Mobile Computing, Volume 6, Issue 5, 2007.

[5] T. R. Sheltami, A. Basabaa, and E. M. Shakshuki, “A3acks: Adaptive Three Acknowledgments Intrusion Detection system for MANETs”, JAIHC, Volume 5, Issue 4, 2014.

[6] E. M. Shakshuki, N. Kang, and T. R. Sheltami, “EAACK— A Secure Intrusion-DetectionSystem for MANETs”, IEEE Transactions on Industrial Electronics, Volume 60, Issue 3, March 2013.

[7] B. Shebaro, D. Midi, and E. Bertino, “Fine-Grained Analysis of Packet Losses in Wireless Sensor Networks”, in 11th IEEE International Conference on SECON, 2014.

[8] S. Buchegger, Jean-Yves Le Boudec, “Performance Analysis of the CONFIDANT Protocol”, in 3rd ACM MobiHoc, 2002.

[9] Osman Khalid, S. U. Khan, “Comparative study of trust and reputation systems for wireless sensor networks”, Journal of Security and Communication Networks, volume 6, Issue 6, 2013.

[10] A. M. Shabut, K. P. Dahal, S. K. Bista, I. U. Awan, “Recommendation Based Trust Model with an Effective Defence Scheme for MANETs”, IEEE Transactions on Mobile Computing, Volume 14, Issue 10, October 2015.

[11] P. Michiardi, R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in MANET”, 6th ACMS, pp. 107-121, Septembeer 2002.

[12] Y. Sun, Z. Han, and K. J. Ray Liu, “Defense of Trust Management Vulnerabilities in Distributed Networks”, IEEE Communications, Volume 46, Issue 2, Februray 2008.

[13] L. Raja, Dr. S. S. Baboo, “An Overview of MANET: Applications, Attacks and Challenges”, IJCSMC, Volume 3, no. 1, pp. 408-417, 2014.