ISSN 2347 - 3983
Volume 8. No. 9, September 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter39892020.pdf
https://doi.org/10.30534/ijeter/2020/39892020

Performance Analysis and Identification Malicious nodes in the MANET using Trust Based and Auditor Based Methods

Lankapalli V. Ramesh[1*] , Chettiar R. Bharathi[2]
[1]Dept. of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu. & Dept. of Computer Science and Engineering, ALIET, Vijayawada, A.P, India.
[2]Dept. of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India.

ABSTRACT

In this communication, we have analyzed the performance of MANET network by adopting the trust based and the auditor based mechanisms with this we are able to identify the malicious nodes in the network. With the incorporation of performance improved watchdog in the MANET, overall network performance is improved in terms of security and the energy effectiveness. The two mechanisms are involved in the performance improved watchdog to identify the malicious nodes in the network, i.e., in primary level we have combined one-hop with auditor node and in the secondary level we have placed an active watchdog. Because of this to level mechanism all the malicious nodes in the MANET are effectively identified and the security of the system is improved.

Key words: MANET, watchdog, WSN, malicious nodes, auditor node.

1. INTRODUCTION

MANET has emerged into many wireless communication applications because of its great ability and potential. MANET topology is complex in nature since the mobile nod s interconnected across multihop communication paths wher e mobile nodes determine the topology[1-4]. Because of MANET topology dynamic nature the probability of malicious nodes is very high. The primary challenges in the MANET is improving the energy effectiveness and improving the network security.

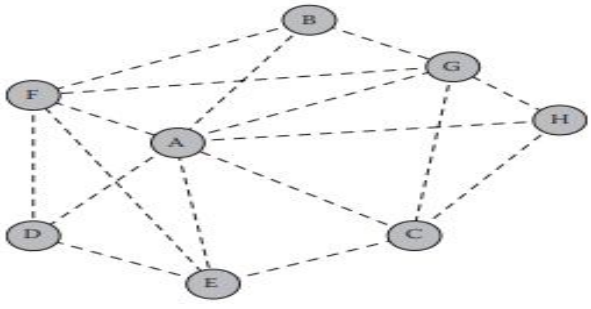

Figure 1: MANET sample model

MANETs are especially susceptible to numerous forms of attacks and threats to security due to maximum sovereignty of the user nodes and absence of any centralized infrastructure. The integration of credibility- and trust-based structures into MANET will help overcome these problems. In a MANET, both nodes may be local, because there is no n etwork connectivity or network back-haul. The network energy effectiveness and security primarily depends on the how effectively we can identify the malicious nodes in the topology. There are so many mechanisms like trust based, audit based and credit based. Active watchdog comes under trust based mechanism to identify the malicious nodes in the network.

In promiscuous mode,watchdog overhears themessage sent b y its neighbors. If it finds any data transmitting anomalies or a malicious data from a neighbor, it may identify the neig hbor as misbehaving.

Condition is generated by taking an extra hop of traversal in which the hostile nodes appear to drop their own packet s while the auditor node attempts to key out nodes that are hostile contributing to their eventual removal. Wireless con nections may be prone to erratic node motions in Mobile A d Hoc Networks (MANET), contributing to regular bond er rors and unexpected topology adjustments. Maintaining the network connection in MANETs can therefore be diffi cult.Mobility control is a significant problem in ad hoc mobi le networks (manets), owing in part to rapidly evolving to pologies of the network[5-8].

A monitor that detects misbehaving nodes and a pathratin g system that allows routinprotocols to stop certain nodes.Th e two methods used to identify and minimize routing misbeh avior are Monitor and Path rate.

The Watchdog identifies nodes that are misbehaving by hold ing a buffer of packets that have just been received. The Deb ugger then tries to check if the next node has already trans mitted a packet by overhearing the adjacent nodes transmiss ions.The Monitor extracts the packet from its buffer as it c oncludes that the next node has forwarded the packet[9-12].

The safeguard system consists of multiple modules, each monitoring module having a different role. The larger t henumber of modules, the greater the amount of resource on

thenode. A likelihood distribution is believed to obey the cr edibi-lity equation.

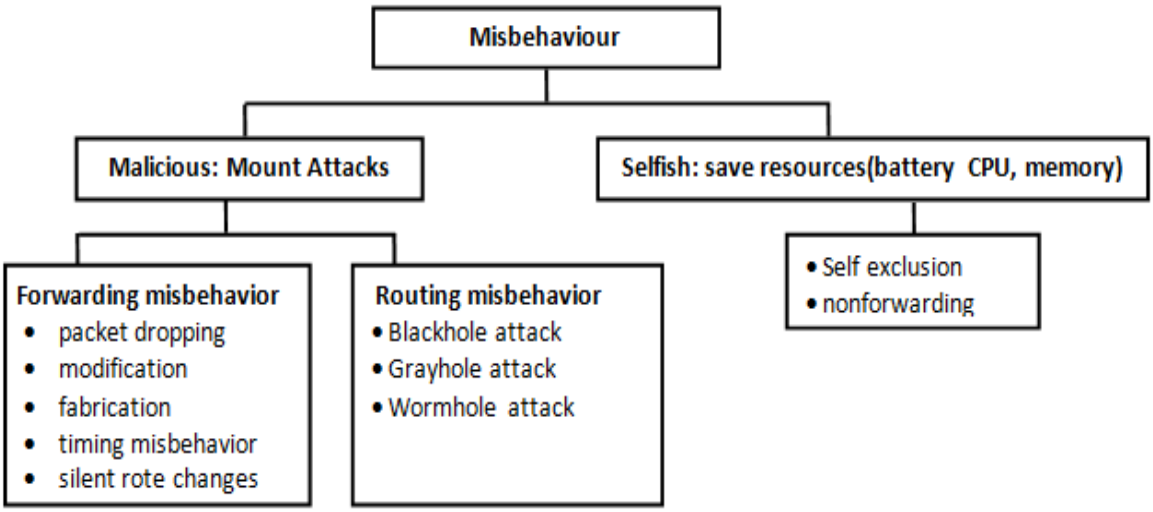

Figure 2: Node's misbehavior in MANET.

2. Related Work

The Watch dog technique is a critical building block for several confidence schemes built to protect wireless sensor networks (WSNs). Unfortunately, this form of procedure requires a great deal of energy and thus effectively reduces WSN's lifetime. The comparison of a transaction is not clear in the case of credibility schemes for MANETs because of the restricted observability and detectability of a mobile node. To track misbehaviour, nodes promiscuously overhear their neighbours conversations.

The part used for this form of monitoring is named Watchdog[9], Monitor [10], or Neighbour Watch[11-12]. Wireless channel instability and energy conservation are the key problems for watchdog systems. Every monitor is located so close to its goal node that communications require minimal resources. In the other hand, mission frequencies are chosen according to the trust worthiness of the goal nodes. the lower frequency of the activities is appropriate when the goal nodes are secure. This saves electricity by cutting back on transmission numbers. The findings also shown effectively that our watchdog optimization strategies will save at least 39.44 percent of energy without losing any reliability (less than 0.06 in terms of confidence precision and robustness), including in certain instances improving safety against some assaults. Several monitoring issues have been found in, such as the challenge of unambiguously detecting that a node is not transmitting packets in the face of collations or in the cases of insufficient transmission capacity.

The watchdog function in CORE is focused on the promiscuous style of wireless node device operations. Moreover, by ranking the end-to-end link the nodes will determine the outcome of a transaction. CONFIDANT utilizes passive acknowledgement not only to check that a node can forward packets, but also as a way of detecting when a packet has been illegitimately changed before forwarding. Marti et al.[13] suggested watchdog and path ratter components for minimizing routing misbehaviour. They found improved performance in MANETs by complementing the DSR protocol with a watchdog for detecting rejected packet forwarding and a path rate for confidence management and routing procedure, ranking any path used.

This makes any node on its routing path to stop malicious nodes. Watchdog measures a node's wrong doing by copying packets to be transmitted to a buffer and tracking the adjacent nodes actions against such packets. Promiscuously the inspector snoops to verify whether the nearby nodes forward the packets without alteration. If the snooped packets fit those in the control node buffer, they will simply be discarded. The packets that persist past a specified among of time in the control node buffer are marked as having been dropped or charged. The node responsible for transmitting the packets would then be identified as a suspect node. If a specified threshold value increases the amount of such failures to forward packets, the guilty node would be marked as a malicious node. Knowledge regarding hazardous nodes is forwarded to the feature pathrater for use in path evaluation [14].

3. Proposed Method

The proposed framework utilizes the Active Watch dog methods for MANET. This procedure is utilized to adjust vitality proficiency and security as far as trust exactness. In this powerful Watch dog enhancement strategy the data sends from source to destination node in the way huge numbers of the nodes are accessible. The neighbour or closest node is considered for data

transmission that is selected Active Watch Dog node with the goal to decrease the consumption of power and increasing security. This Watch dog is called as a Active Watch dog as it continuously monitors all the nodes transactions during data communication.

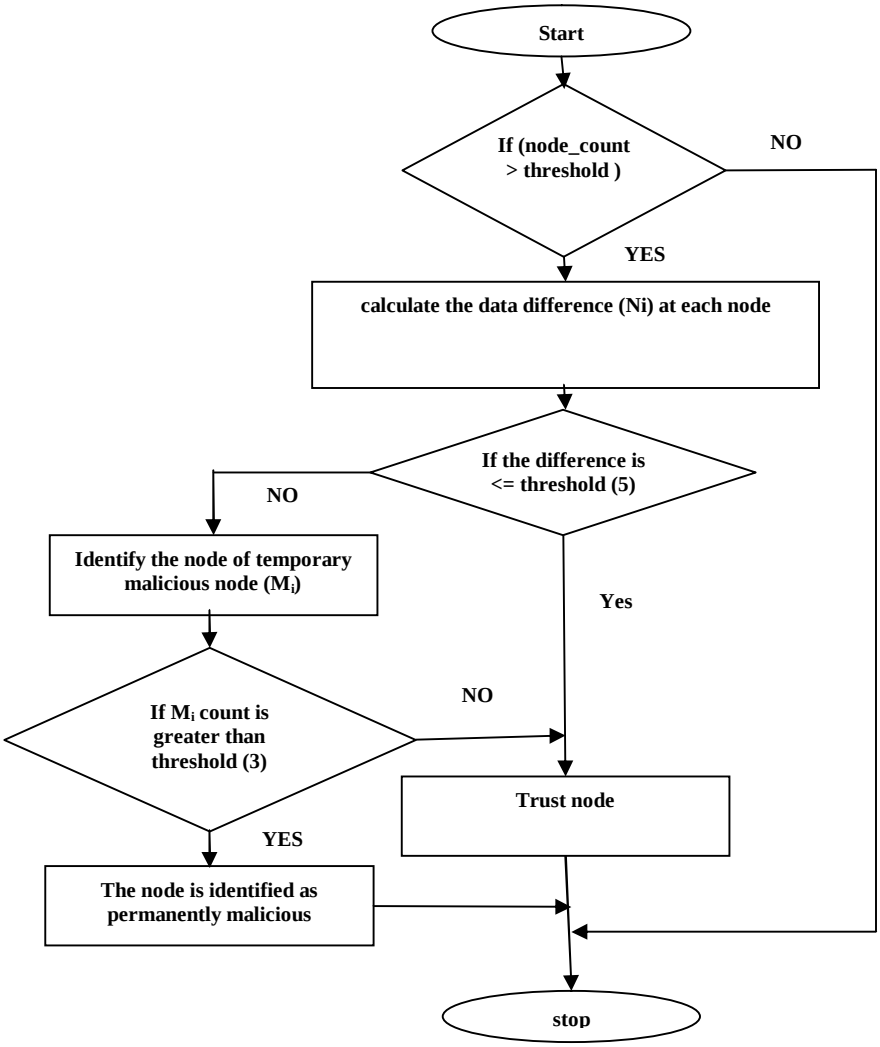

Figure 3: performance improved active watchdog algorithm flowchart.

Initially when a MANET is established, the nodes in the network are dynamic in nature and then the administrator nodes are selected for key generation and maintenance. Among the nodes initially a node having high computational power and energy efficiency is considered as Active Watchdog node and when the communication is initiated, the node will calculate the data packets received by the node and send to neighbor nodes as

Data Transferred (N_i) = Data Received – Data Send to Neighbor node. (1)

Here N_i represents specific node i.
If there is any change in the data transferred level, the node is marked as malicious node and the remaining nodes are certified as trusted nodes. A node whose data transferred rate is less than '5' is certified as trusted nodes. After the communication is completed, the network marks all nodes as trusted or malicious nodes.

The Active watchdog node will be dynamically changed for every transaction and the data maintained by the Active watch dog node should be transferred to the new Active Watchdog node before leaving the MANET. The watch dog node records the malicious activities caused by several nodes and those nodes are not considered from next communications. Extreme objective is to lessen the power consumption by Watch dog.

4. RESULTS AND DISCUSSIONS

4.1. Auditor based

The test was performed in the simulator at NS2. A distincti on was made between the approaches introduced and the pro cedures used during the audit. The findings are illustrated gr aphically below based on the research which focuses on the packet distribution ratio. In the experiment,three approaches were analysed. It includes; Normal Auditor Process process Auditor & One Hop (AOH) system.

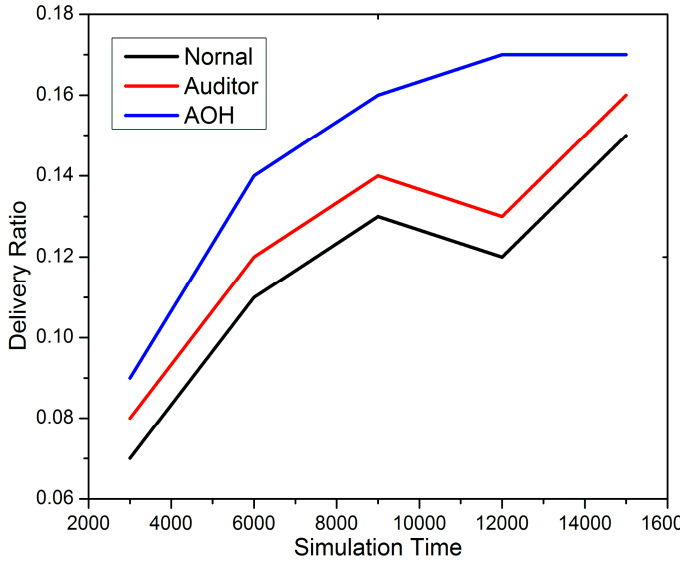

Figure 4: Delivery ratio: 10% malicious nodes.

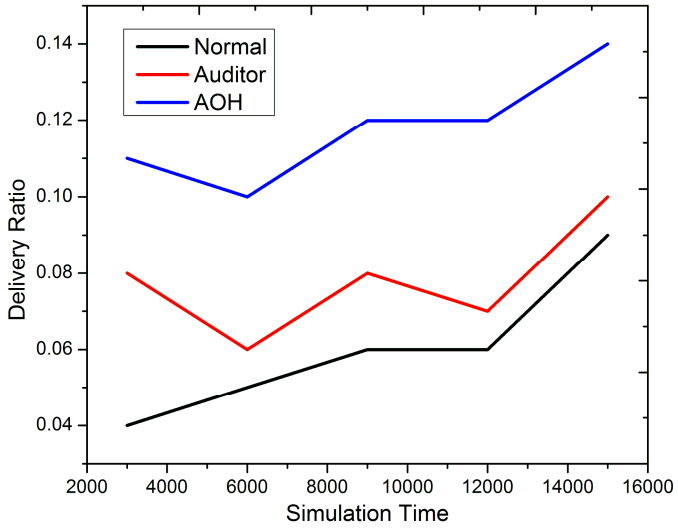

Figure 5: Delivery ratio: 20% malicious nodes.

The distribution ratio is the percentage of the message trans mitted to the message produced.

$$Deliveryratio = \frac{Number\ of\ messages\ delivered}{Number\ of\ messages\ created} \qquad (2)$$

In Figure 3 and Figure 4, the three strategies are compared

and contrasted respectively with 10 percent and 20 percent malicious nodes. With the rising amount of malicious nodes, the amount of packet droppings is growing. The AOH approaches thus demonstrates significantly improved distribution efficiency than other approaches. In the proposed AOH process, the pause in data transmission between the nodes is minimized and is shown in the figure below.

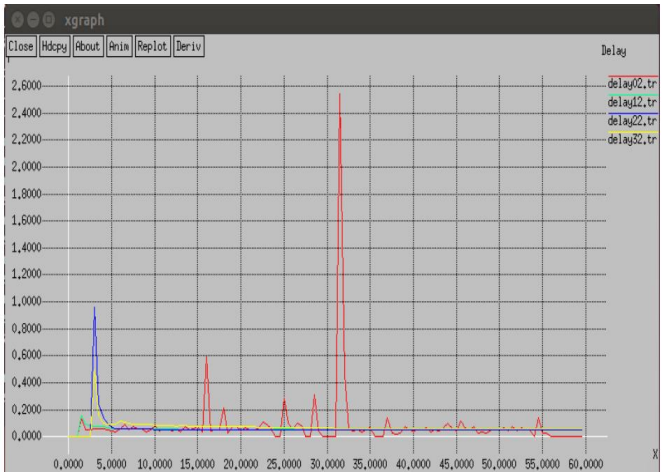

Figure 6: Delay in data transfer.

The two mechanisms are involved in the performance improved watchdog to identify the malicious nodes in the network, i.e., in primary level we have combined one-hop with auditor node and in the secondary level we have placed an active watchdog. The approach suggested eliminates the failure of the packets during contact. Any node essentially has the auditor and on e hop method if it has forwarded the packets to next nodes w ithout any miscellaneous intervention. Reduction of packet l oss rate is seen in the figure below.

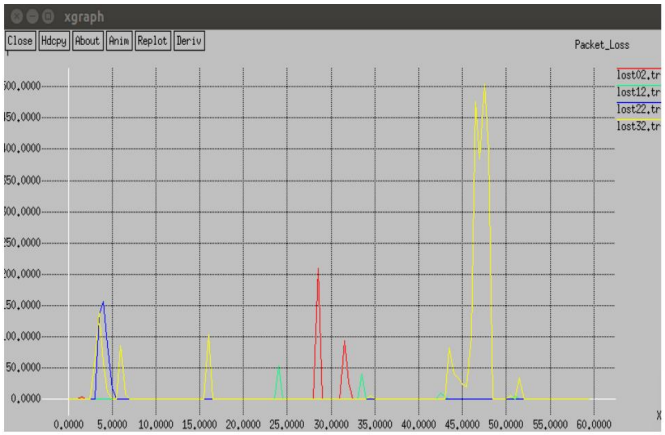

Figure 7: Packet loss reduction.

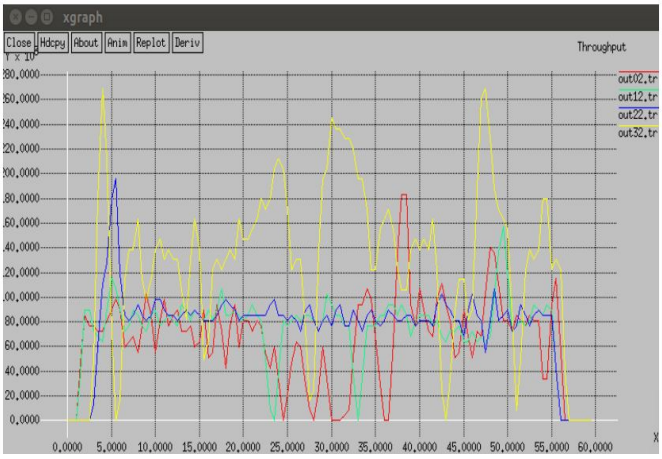

Figure 8: Throughput level.

The suggested system efficiency is higher than the current methods. The findings indicate that the AOH approach suggested demonstrates greater and better efficiency than conventional methodologies.

4.2. Trust based

The proposed method is implemented in NS2 and the proposed watchdog method is implemented which provides security to the data and identifies the malicious nodes in the MANET for secure data transmission. The parameters used for establishing a MANET is depicted in Table 1.

Table 1: Experimental Parameters

PARAMETER	VALUES
Simulation time	5 mins
Topology size	1000 X 1000
No. of nodes	10
No. of clusters	2
Node mobility	0 to 20m/sec
Routing Protocol	DSDV
Frequency	11 MHz
Traffic type	CBR
MAC	IEEE 802.11
Mobility model	Random Waypoint
Max. no. of packets	10000
Pause time	10sec

The overall communication overhead of the proposed active watch dog method is compared with the traditional watch dog method and the results are depicted in figure 9.

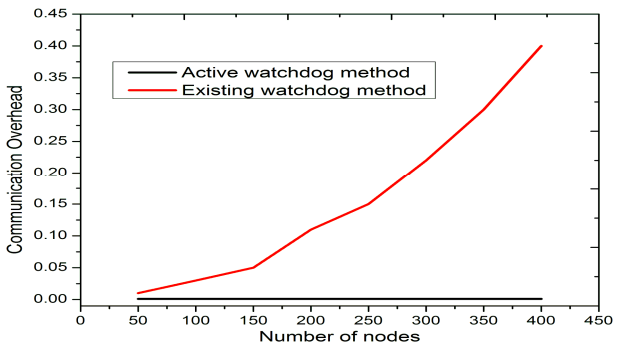

Figure 9: Communication Overhead levels.

After the MANET is established and the watch dog node is selected, the identification rate of the malicious nodes are depicted in Figure 10.

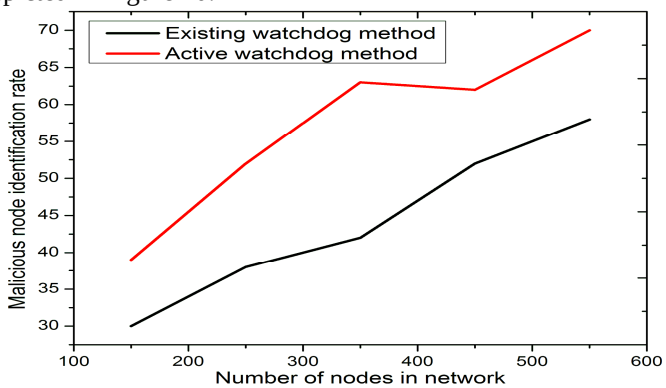

Figure 10: Active Watch dog system identification rate.

The proposed active watch dog method effectively identifies the malicious nodes in the network. As all nodes are trusted nodes, the packet delivery rate in the proposed method is high as shown in Figure 11.

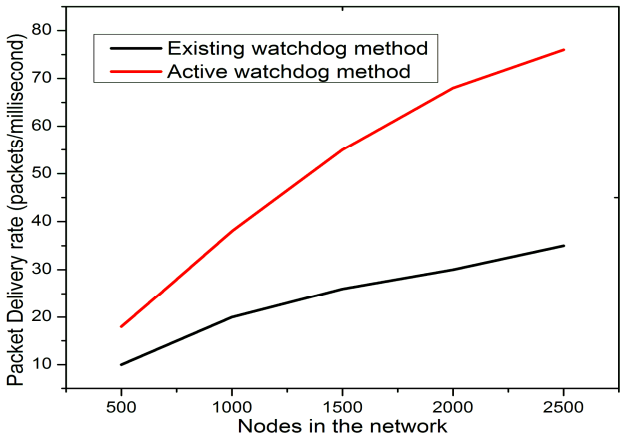

Figure 11. Packet Delivery Ratio.

The energy consumption rate of the proposed method is very less when compared to traditional methods. The energy consumption rate is depicted in Figure 12.

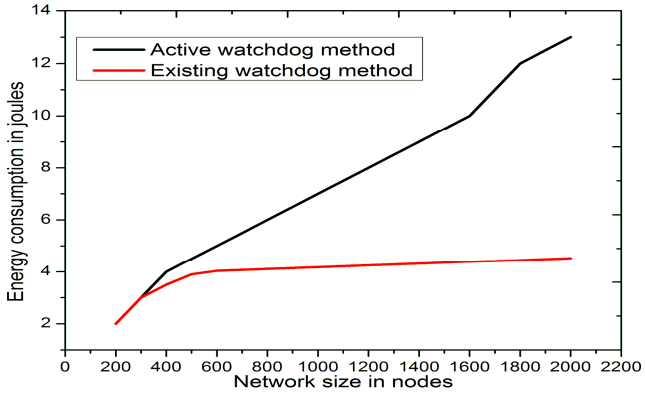

Figure 12: Energy Consumption Ratio.

The data security level of the proposed method is illustrated in Figure 13.

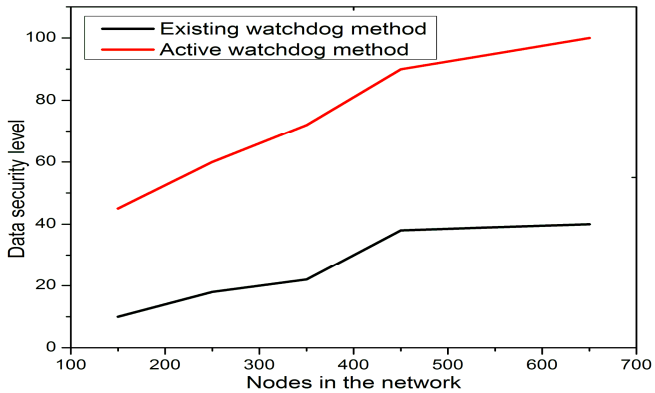

Figure 13: Data Security Level.

5. CONCLUSION

we have improved the watchdog performance in the MANET network which is able to identify the malicious nodes in the network. With the incorporation of performance improved watchdog in the MANET, overall network performance is improved in terms of security and the energy effectiveness. The two mechanisms are involved in the performance improved watchdog to identify the malicious nodes in the network, i.e., in primary level we have combined one-hop with auditor node and in the secondary level we have placed an active watchdog. Because of this to level mechanism all the malicious nodes in the MANET are effectively identified and the security of the system is improved.

REFERENCES

1. Anto Ramya S.I, **Mobile ad-hoc Netwoek Topology and its Algorithms**, *International Journal of Trend in Research and Development*, 2(5), Pp 16-21, 2015.
2. Narendra Reddy .P, Vishnuvardhan C.H, Ramesh.V, **Routing Attacks in Mobile ad-hoc Networks**, 2(5), pp 360-367, 2013.
3. O.Kachirski, R. Guha, **Effective Intrusion Detection Using multiple sensors in Wireless ad-hoc Networks**, *International Conference on System Sciences*, 2003.
4. S. Marti, T.J. Giuli, K. Lai, and M.Baker. **Mitigating routing misbehavior in mobile ad hoc networks,** *6th MobiCom, Boston*, Massachusetts, 2000.
5. Evgeniy Ivanovich Trubilin, Svetlana Ivanovna Borisova, Vladimir Ivanovich Konovalov, Mikhail. **Experimental Studies of Parameters of Pneumatic Slot Sprayer**, *International Journal of Emerging Trends in Engineering Research*, 8(1), 2020.
6. Karti kumar Srivasta, Avinash Tripathi, Anjnesh kumar Tiwari, **Secure Data Transmission in MANET Routing Protocol,** *International Journal of Computer Technology& Applications*, 3(6), pp 1915-1921, 2012.
7. R. Bhuvaneshwari, G. Nalina keerthana, A. Rachel Roselin, **Improving Selfish Node Detection In MANET Using A Collaborative Watchdog**, *International Journal of Advanced Research Trends in Endineering and Technology*, vol 3, No 15, pp 17-21, 2016.
8. Harold Robinson, M. Rajaram, E. Golden Julie, S. Balaji. **Detection of Black Holes in MANET Using Collaborative Watchdog with Fuzzy Logic**, *International Journal of Computer and Information Engineering*, Vol 10, No 3, pp 622-628, 2016.
9. Sun B, Guan Y, Chen J, Pooch U. **Detecting black hole attack in mobile ad hoc networks**, *IEEE Transactions on Vehicular Technology*, 490-495, 2003.
10. Buttyan L, Hubaux JP. **Stimulating cooperation in self organizing mobile ad hoc networks**. *ACM/Kluwer Mobile Netw.* PP-579-592, 2003.
11. Zhong S, Chen J, Yang YR. **Sprite: A simple cheat-proof, creditbased system for mobile ad-hoc networks**. *In Proc. IEEE INFOCOM Conf* , PP-1987- 1997, 2003.
12. Balakrishnan K, Deng J, Varshney P. **TWOACK: Preventing selfishness in mobile ad hoc networks**. *In Proc. IEEE Wireless Commun. Netw. Conf* , pp: 2137-2142, 2005.
13. Hennadii Khudov, Irina Khizhnyak, Fedor Zots, Galina Misiyuk, Oleksii Serdiu. **The Bayes Rule of Decision Making in Joint Optimization of Search and Detection of Objects in Technical Systems**, *International Journal of Emerging Trends in Engineering Research*, 8(1), 2020.
14. JKR Sastry, M Trinath Basu, **Multi-Factor Authentication through Integration with IMS System**, *International Journal of Emerging Trends in Engineering Research*, 8(1), 2020.