RESEARCH ARTICLE

DOI: 10.34256/ijcci2211

International Journal of Computer Communication and Informatics

Predicting Malicious Node Behavior in Wireless Network Using DSR Protocol and Network Metrics

A. Ganesan [a,*], A. Kumar Kombaiya [b]

[a] Department of Computer Applications, Hindusthan Arts College, Coimbatore–641028, Tamil Nadu, India.

[b] Department of Computer Science, Chikkanna Government Arts College, Tirupur-641602, Tamil Nadu, India.

* Corresponding Author: ganesana102@gmail.com

Received: 12-02-2022, Revised: 20-04-2022, Accepted: 28-04-2022, Published: 03-05-2022

Abstract: This paper describes a set of network metrics are helpful to predict behavior of malicious node in wireless network. The Network and internet is the device in which multiple people can communicate with each other through the wired or wireless media. Nowadays, Internet of Things, Mobile, vehicular, and wireless ad hoc networks all merge into one shared network. These networks are often used to send receive confidential data and information. The unauthorized or malicious node misuse these secrete information. With a rise in rogue nodes, network performance will suffer. A rogue node in the network can cause variations in network metrics including the packet dropping percentage, throughput, latency, energy consumption, and average queue duration. This behavior used to identify the malicious node.

Keywords: Malicious Node, DSR, Throughput, Latency, NS2, Packet Delivery Ratio, Energy Consumption, Intrusion Detection System.

1. Introduction

The two things we need most in our daily lives are a computer network and the internet. To pass the personal information or official information quickly to the essential place network or internet is one of the most powerful media. The network is used as wired networks and wireless networks. Data packets are basic entities in all types of networks. Security of network implies security of data packets. The enormous attacks from networks or the internet increase day by day. The quality of network service and security is becoming more issue; hence it requires a powerful network monitoring system, traffic analysis, and secured distribution engine for the network application.

A group of wireless mobile nodes that form a temporary network without the use of a centralized access point or centralized administration is known as a mobile ad hoc network. In this research work we employed five network metrics to identify behavior of malicious node.

2. Performance Parameters

In this research paper, five performance parameters are used to assess the network's performance in the event of DSR without an attack and DSR with an attack. They are Throughput, Packet Dropping Ratio, Energy consumption, Latency, and Average queue length. The following table shows the value of these metrics for the network simulator time 10, 20, 30 and 40 ms with malicious and without malicious node using NS2 tools [1-3].

Table 1. No. of Node: 70 No. of Packet: 60 Source: node 2 Destination: 65 With Malicious Node

simulator-time/Network- Metric	Queue- Length	Throughput	Packet-Drop	Energy consumption	Latency
0	9.25	9.25	10	10	10
10	9.43	9.48	9.94	9.95	9.97
20	9.5	9.49	9.81	9.87	9.92
30	9.58	9.5	9.68	9.82	9.84
40	9.66	9.51	9.59	9.75	9.78

Table 2. No. of Node: 70 No. of Packet: 60 Source: node 2 Destination: 65 Without Malicious Node

simulator- time/Network-Metric	Queue-Length	Throughput	Packet-Drop	Energy consumption	Latency
0	9.25	9.25	10	10	10
10	9.43	9.38	9.87	9.87	9.97
20	9.51	9.43	9.76	9.83	9.92
30	9.61	9.51	9.64	9.78	9.84
40	9.69	9.56	9.54	9.7	9.78

2.1 Throughput

It refers to the volume of data sent through a communication network in a particular time from one node to another. The amount of data transferred between multiple locations over a given time period is tabulated to determine throughput, which typically results in the unit of bits per second (bps), which has since evolved into bytes per second (Bps), kilobytes per second (Kbps), megabytes per second (Mbps), and gigabytes per second (Gbps) . Numerous elements, including the limitations of the underlying analogue physical medium, the computing power available to system components, and end-user behavior, can influence throughput [4, 5]. The network throughput is computed as

$$\text{Network Throughput} = \Sigma^{n}_{i=1} \quad \text{Total number of packets} / T_{tp} - T_{r}.$$

The Ttp indicates the quantity of packets sent, and the Ttr indicates the quantity of packets received. Bits per second are used to measure throughput capacity. The time needed to transport a request from a source to a destination or a response from a destination to a source is represented by this throughput measure. The overall reaction time that each node experiences is significantly influenced by this value. It is based on the amount of data necessary for the request and answer as well as the transmission's quality.

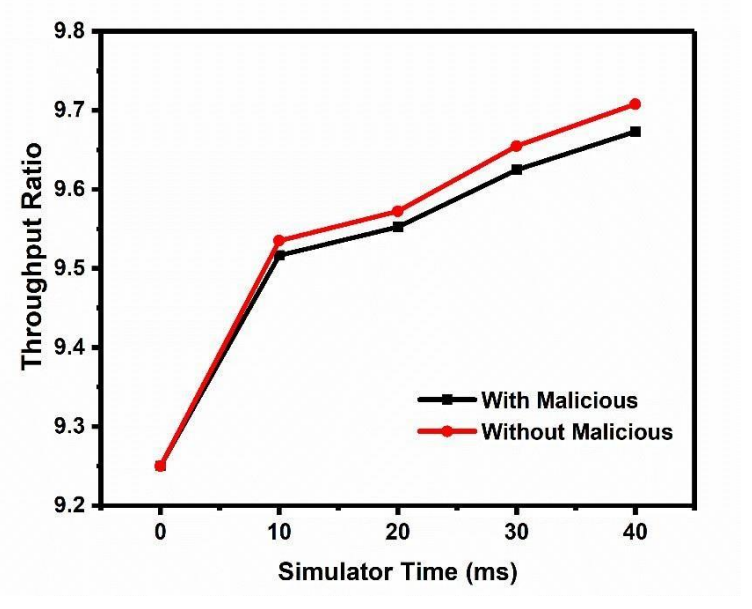

Figure 1. Throughput ratio for various simulator times in 200 nodes

2.2 Packet Dropping Ratio

When one or more data packets going over a network are unable to reach their destination, this is known as a packet loss event. Network congestion or data transmission failures

in a wireless network are the two main causes of packet loss. A packet dropping rate is calculated as a percentage of lost packets compared to transmitted packets. These are metrics calculated as

Packet Dropping = (Number of Packets sent – Number of Packets Received) ×100

When a specific router gets a packet and decides not to deliver it to the next hop, the packet is lost. The cause of packet loss may be natural or artificial interference. "Dropping" is the term for this type of packet loss [6-8].

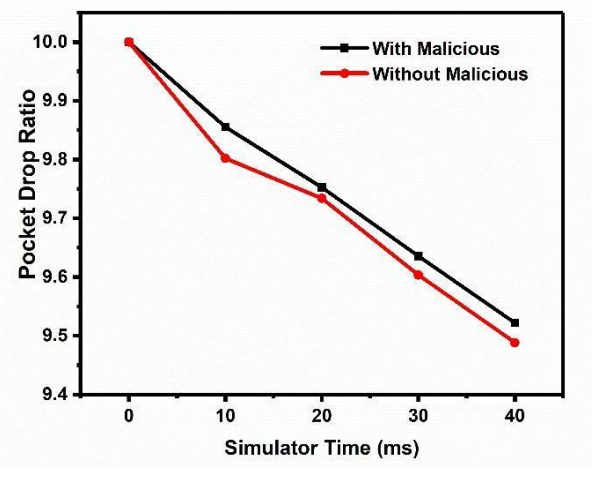

Figure 2. Pocket dropping ratio for various simulator times in 200 nodes.

2.3 Energy Consumption

The switching, transmission, and access networks all utilize energy, which is the amount used by a single node to transport a packet [9].Overconsumption of energy can result from a number of circumstances, including: re-transmissions, mobility.

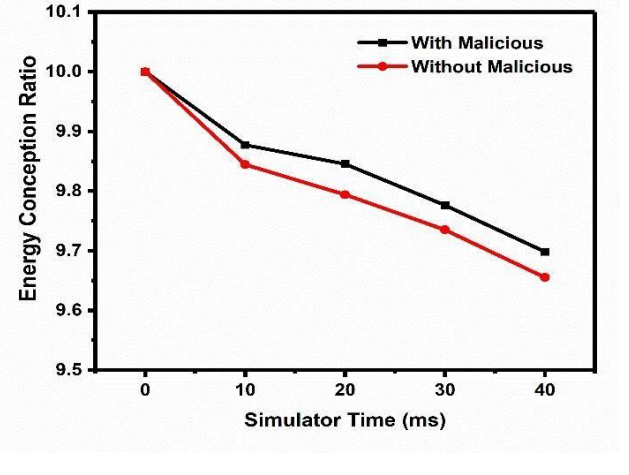

Figure 3. Energy conception ratio for various simulator times in 200 nodes

The main problem of the host which is in a wireless network is energy consumption node will take more energy while its data transmission [8]. It wastes its resources due to delays in packet transmission and packet dropping. The encryption of the packet will take more energy consumption. If the distance is quite far, the transmission in one hop uses more energy. Re-transmissions, collisions, idle listening, control packets, and overhearing all affect how much energy is used. The energy consumption will be increased when the malicious node exists.

2.4 Latency

Latency, also known as delay, is the amount of time it takes for a message to be delivered in its entirety from the source to the destination over a network, beginning with the time the first bit of the message is sent out and ending with the time the last bit of the message is received at the destination. Low-Latency-Networks are network connections that experience brief delays, whereas High-Latency-Networks are network connections that experience significant delays.

Any network communication that experiences high latency develops bottlenecks. It effectively reduces the communication network's bandwidth by preventing data from fully utilizing the network channel. Depending on the cause of the delays, the impact of latency on a network's capacity may be momentary or permanent. Ping rate, another name for latency, is a millisecond-based unit of measurement (ms).

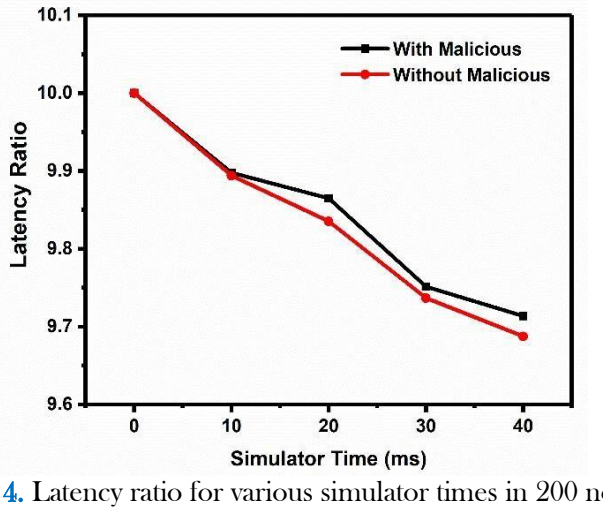

Figure 4. Latency ratio for various simulator times in 200 nodes

2.5 Average Queue Length

Queuing in a network directly relates to congestion. Various queuing techniques are used to manage the Buffers on network devices. Effective queue management can reduce dropped packets and network congestion while also enhancing network performance.

In Drop-head queuing technique, packets drop at the head of the queue, and in Drop-tail queuing technique, packets Drop at the tail of the queue. The most fundamental queue

management method is called FIFO (first-in, first-out), where packets are processed in the order that they enter the queue. However, more sophisticated techniques, such as the priority queuing scheme, employ numerous queues with various priority levels so that the most crucial packets are dispatched first.

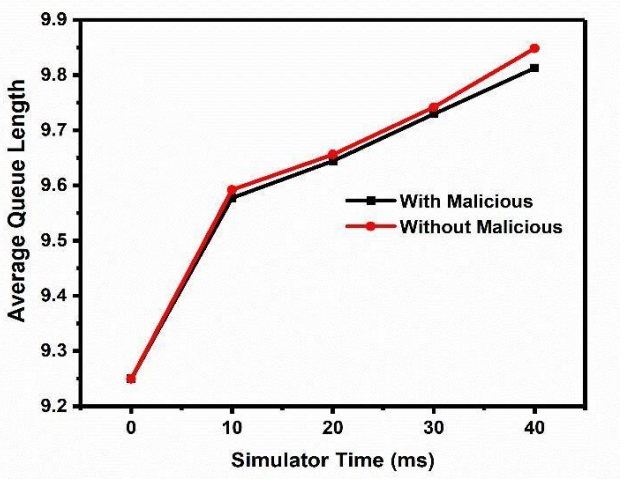

Figure 5. Average queue length for various simulator times in 200 nodes

3. Scenario for Simulation

We use the NS-2 Simulator with DSR protocol to develop the wireless network performance evaluation model [10-12]. To imitate node movement, the random way approach is used. Within the simulated area, each node begins moving at a random speed from its source node to its destination node. 10 nodes are first placed for the simulations in random locations. After that 20, 30, and 40 node has been created for the simulation. We have created these environments with malicious nodes and without malicious nodes and a DSR routing protocol is implemented.

Table 3. Parameter used in the simulation

Parameter	Value
Channel type	Wireless channel
Number of nodes	200
Pulse time	0 ms,10 ms, 20 ms, 30 ms, and 40 ms
Traffic type	CBR
Data Payload	512 bytes
MAC Type	802.11
Node placement	Random
Mobility	Random way
Area simulation	1000m*1000m

4. Result Analysis

This effort aims to assess the effects of malicious nodes and gauge network performance using the DSR routing protocol at various node densities both with and without malicious nodes.

To find the performance of the wireless network with DSR protocol under malicious attack we included a few nodes as malicious nodes. Initially, we measured Throughput, Packet Dropping Ratio, Energy consumption, Latency, and average queue length by varying number of nodes [5]. We fix few malicious nodes with pause time 10 m/s, 20 m/s, 30 m/s and 40 m/s. The DSR routing protocol's throughput with more nodes is depicted in Figure 1. In comparison to regular DSR, malicious attacks on throughput are less frequent.

As Figure 2. shows the packet Dropping Ratio of a wireless network using DSR protocol with and without malicious node. As the malicious node increases the packet dropping ratio but takes the value Packet Dropping ratio without malicious node 9.4328 for 200 nodes at 40 m/s pause time. The result shows without malicious nodes have a low packet dropping ratio for 200 nodes.

The Figure 3. shows the Energy consumption of wireless networks using DSR protocol with ad without malicious nodes. As the malicious node increases the Energy consumption but takes the value Energy consumption without malicious node 9.67 for 200 nodes at 30 m/s pause time. The result shows without malicious node has low energy consumption.

The Figure 4. shows the Latency of wireless networks using DSR protocol with and without malicious nodes. As the malicious node Latency level is high (9.78) for 200 nodes at 20 m/s pause time. But taking the value of latency without malicious node 9.77 for 200 nodes has a low value

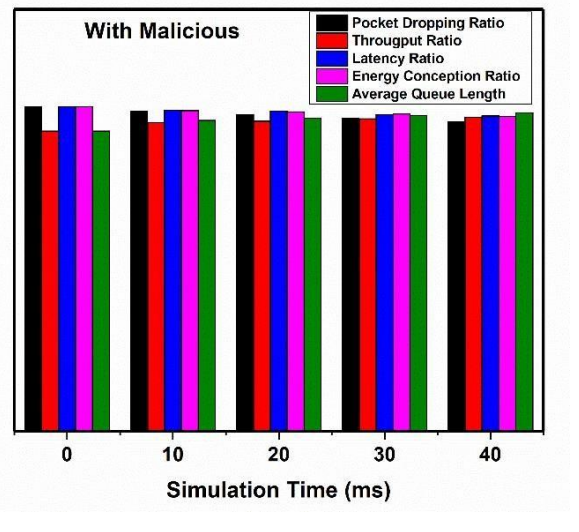

Figure 6. Simulation time Vs various parameters for with Malicious

The Figure 5 shows the Average Queue Length of a wireless network using DSR protocol with and without malicious nodes. With the malicious node [13] increase the packet transmission time due to congestion {traffic) problem. Its average time is 9.55 for 200 nodes at 10 m/s pause time. But taking the value of average queue length without malicious node 9.65 has a high value.

The Figure 6 shows a comparison of important network matrices such as throughput, Packet Dropping Ratio, Energy consumption, Latency, and Average queue Length of a wireless network using DSR protocol with a malicious node for 200 nodes at 0 ms, 10 m/s, 20 m/s, 30 m/s and 40 m/s simulator time. The Figure 7 shows a comparison of network matrices of a wireless network using DSR protocol without malicious nodes for 200 nodes at different simulator times. From the comparison graph [14, 15], we can observe the malicious node consisting of the network always decrease the performance of the network.

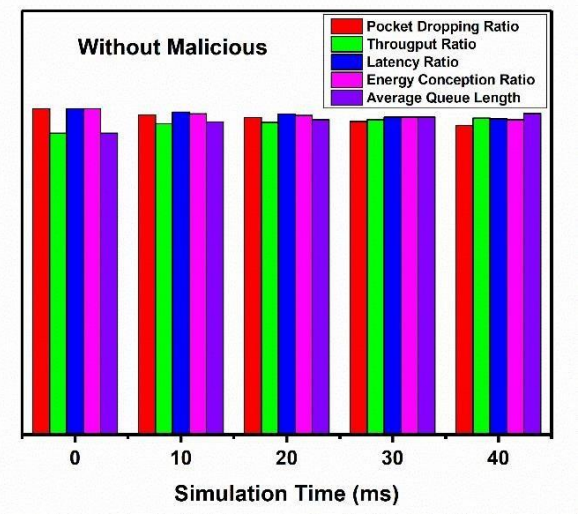

Figure 7. Simulation time Vs various parameters for without Malicious

5. Conclusion

The attack made on networks has risen dramatically for many years. Due to the unlimited access to and use of software written and uploaded by technical experts. Network disruption is caused by several types of directed attacks. Therefore intrusion detection system is considered to use one of the best technologies to detect the attack and network performance. With this method, we are able to determine the effects of a rogue node on the DSR routing protocol at various node densities subject to an attack from a malicious node. The outcome demonstrates that DSR without a malicious attack performs better in terms of throughput, packet dropping ratio, energy consumption, latency, and average queue length. It has been discovered that the inclusion of malicious nodes causes the DSR routing protocol's network performance to decrease.

References

[1] The Network Simulator - ns-2. https://www.isi.edu/nsnam/ns/index.html

[2] Fall K., & Varadhan K, (2011). The ns Manual (formerly ns Notes and Documentation), https://www.isi.edu/nsnam/ns/doc/ns_doc.pdf

[3] Chung, J., & Claypool, M. (2002). NS by example. *Worcester Polytechnic Institute, Computer Science*. http://nile.wpi.edu/NS/

[4] Wei, D.X., (2005). Speeding up NS-2 scheduler. http://netlab.caltech.edu/projects/ns2tcplinux/ns2patch/ns2patch.htm

[5] Das, S.R., Castaneda, R., Yan, J., & Sengupta, R., (1998). Comparative performance evaluation of routing protocols for mobile, ad hoc networks, *In Proceedings 7th International Conference on Computer Communications and Networks,* IEEE, 153-161. https://doi.org/10.1109/ICCCN.1998.998772

[6] Sahu, P., Bisoy, S.K., & Sahoo, S., (2013). Detecting and isolating malicious node in AODV routing algorithm, *International Journal of Computer Applications*, 66 (16), 8-12.

[7] Khandakar, A., (2012). Step by step procedural comparison of DSR, AODV and DSDV routing protocol, *4th In International Proceedings of Computer Science &Information Techenology*, 40 (12), 36-40.

[8] Baliga, J., Ayre, R., Hinton, K., & Tucker, R.S., (2011). Energy consumption in wired and wireless access networks, *IEEE Communications Magazine*, *49*(6), 70-77. https://doi.org/10.1109/MCOM.2011.5783987

[9] Rohini, R., & Gnanamurthy, R.K., (2016). A Simple and Efficient Malicious node detection system for improving the performance of the wireless sensor networks, *International Journal of Applied Engineering Research*, 11(1), 396-400.

[10] Singh, R., Singh, J., & Singh, R. (2017). Fuzzy based advanced hybrid intrusion detection systemtodetect maliciousnodes inwirelesssensor networks, *Wireless Communications and Mobile Computing,* 2017, 1-14. https://doi.org/10.1155/2017/3548607

[11] Sarigiannidis, P., Karapistoli, E., & Economides, A.A., (2015). Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information, *Expert Systems with Applications,* 42 (21), 7560-7572. https://doi.org/10.1016/j.eswa.2015.05.057

[12] Maleh, Y., Ezzati, A., Qasmaoui, Y., & Mbida, M., (2015). A global hybrid intrusion detection system for wireless sensor networks, *Procedia Computer Science*, 52, 1047-1052. https://doi.org/10.1016/j.procs.2015.05.108

[13] Adnan, A., Kamalrulnizam, A.B., Muhammad Ibrahim, C., Khalid, H., & Abdul Waheed, K., (2014) A Survey on Trust-Based Detection and Isolation of Malicious Nodes in Ad-Hoc and Sensor Networks, *Frontiers of Computer Science (electronic),* 9(2), 280-296. http://dx.doi.org/10.1007/s11704-014-4212-5

[14] Li, Z., Sun, J., Yan, Q., Srisa-an, W., & Bachala, S., (2018). Grandroid: Graph-based detection of malicious network behaviors in android applications, *In International*

Conferenceon Securityand Privacy in Communication Systems, Springer, Cham, 254, 264-280. https://doi.org/10.1007/978-3-030-01701-9_15

[15] Rajasekaran, B., & Arun, C., (2018). Detection of malicious nodes in wireless sensor networks based on features using neural network computing approach, *International Journal of Recent Technology and Engineering,* 7(4), 188-192.

Funding

No funding was received for conducting this study.

Conflict of interest

The Authors have no conflicts of interest to declare that they are relevant to the content of this article.

About The License