IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MALICIOUS NODE DETECTION

[1]S Balaji ,[2] Dr. R.PUSHPAVALLI, M.Tech., Ph.D.,

[1]Student of M.E Communication System, [2]Associate Professor.,ECE ,

[1]M.E Communication System,

[1]Paavai Engineering College, Namakkal, Tamil Nadu , India

ABSTRACT

There are a lot of inexpensive, tiny sensor nodes in Wireless Sensor Networks (WSN) that can send data. limited memory, limited processing power, low power supply, and short communication range are the limitations of wireless sensor nodes. Due to these limitations, this network is susceptible to numerous attacks, particularly the bwdos_sinkhole_attack attack. A type of attack known as a "bwdos sinkhole attack" involves the hacked node attempting to draw in network traffic by promoting its bogus routing update. A bwdos_sinkhole_attack attack has the ability to initiate spoofing, selective sharing, and removing or modifying routing data, among other impacts. It might also be used to send fictitious data to the base station. In this paper, time-varying in wireless sensor networks, bwdos_sinkhole_attack attack detection technique based on snapshot-based Neighbour-controlled Traffic-centric (TSNT) technology is used to address these issues and enhance service quality. The base station monitors the traffic using the TSNT algorithm, and it keeps track of the list of sensor devices the packet has passed through over time. The presence of bwdos_sinkhole_attack is identified from this list using a snapshot of the WSN captured at different times. In parallel, the base station receives assistance from a reliable outside source within the WSN network to identify the bwdos_sinkhole_attack attack through message digest hash-based data integrity verification. The experimental outcome demonstrates that, in comparison to other current techniques, the suggested method efficiently detects bwdos_sinkhole_attack.

Keywords: Network vulnerability, Bwdos_sinkhole_attack attack, Fake data, Dropping, Service quality

1.INTRODUCTION

One of the most well-known types of networks is the wireless sensor network (WSN), which is utilized in a variety of applications, including industrial surveillance, environmental remote sensing, health monitoring, and area surveillance. It is possible to use the WSN in an unsecure, hostile work environment. sensors that monitor the surroundings and send the data they collect back to the base station. Due to their inherent characteristics, WSNs are vulnerable to many security threats. Such communication encourages data leaks, which lead to security lapses. As such, the primary difficulty in WSNs continues to be security. Many sensor networks have relatively basic routing protocols, which makes them vulnerable to network attacks most of the time. The wormhole attack, black hole assault, hello flood attack, bwdos sinkhole attack, and selective forwarding attack are a some of the WSN's vulnerable security vulnerabilities.

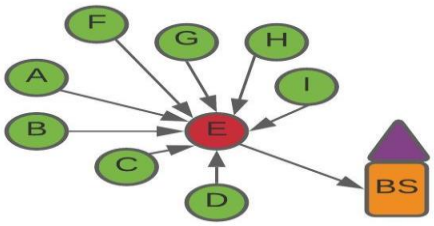

Fig. 1: Bwdos_sinkhole_attack attack in Wireless Sensor Network

An attacker gains access to a device on the network and uses it to launch an attack in the bwdos sinkhole attack. The hacked device attempts to draw all traffic from the closest nodes based on the routing metric used in the routing protocol. The hacked equipment is equipped with a strong radio transmitter capable of taking down a large wide area network. Unaware of this, the adjacent gadget will trick with these devices. A bwdos_sinkhole_attack attack poses a major threat to higher-layer applications by preventing the base station from getting accurate and comprehensive sensed data. Because it is difficult to verify routing information supplied by a device, Bwdos sinkhole attacks are challenging to defend against. The black hole, Sybil, flood, wormhole, and selective forwarding attacks are all carried out by a Bwdos sinkhole assault once it has gained access to a network. Many methods

have been presented by researchers to identify bwdos_sinkhole_attack attacks in WSNs. However, these methods suffer from high-complexity discovery and overhead brought on by the discovery process.

2.LITERATURE REVIEW:

The detection of the bwdos_sinkhole_attack attack on the WSN was resolved by Nithiyanandam et al. [1] using the artificial bee colony (ABC) approach. By comparing the defined device ID in the rule-set, this approach finds the hacked device. By cutting down on the total time required to identify the compromised device, ABC improves both the packet delivery ratio and the packet loss percentage.

One of the finest methods for spotting a bwdos_sinkhole_attack attack in the WSN is artificial intelligence. As a result, in the AODV routing protocol, Singh et al. [2] discovered a bwdos_sinkhole_attack attack based on a neural network. They compared the various parameters of the current methods—the entire simulation run in the MATLAB 2010a environment—such as network load, throughput, and end-to-end delay.

An enhanced Particle Swarm Optimization (PSO) technique for bwdos_sinkhole_attack attack detection was presented by Keerthana et al. [3]. Their efforts enhance the prior PSO method, and the enhanced algorithm's efficacy is evaluated using a simulation. It was determined that, in comparison to the earlier PSO and Ant Colony Optimization (ACO) methods, the enhanced PSO algorithm performs better in terms of packet delivery ratio and message drop.

A survey of various pathways with safety concerns in WSNs, with a primary focus on the Bwdos sinkhole attack, was provided by Tandon et al. [4]. They also provide a range of ways to identify and stop bwdos_sinkhole_attack attacks. The countermeasures used to thwart the bwdos_sinkhole_attack attack are the last ones they cover.

In order to guarantee data integrity during communication, Babaeer et al. [5] proposed a simple, secure way utilizing water-marking techniques and the Threshold Sensitive Power Proficient WSN protocol. When looking for sensor devices for bwdos_sinkhole_attack detection and avoidance, the homomorphic encryption used in this study is rapid, efficient, and low power consumption. The OMNET ++ simulator is used to evaluate the proposed work and determine how well it performs in terms of average power consumption, delay, performance, and packet delivery ratio. The suggested strategy shows the greatest results in these quantifications when compared to the existing methods.

3.EXISTING SYSTEM

Current technological breakthroughs are utilized by modern Information and Communication Technology (ICT)-based apps to stream data in an effort to keep up with the rapidly evolving technological landscape. Accurate, significant, and reliable output from the streaming sensors is necessary for these efforts, especially during dynamic virtual sensing. However, it is crucial to put secure real-time solutions into place to guarantee that the sensing environment is free of any sensor threats or active attacks. Essentially, the secret to predicting possible attacks in active learning is the real-time detection of adversarial attacks/instances during the User Feedback Process (UFP). Additionally, as of the time this work was written, no thorough investigation has been done with an emphasis on adversarial detection from an active machine learning perspective, according to the literature already in existence. As a result, the authors stress the significance of using adversarial attack detection in active learning strategies. Within the framework of this research, an attack is defined as any activity that modifies the data or learning system using a UFPThreat driven model. In order to do this, we purposefully subjected the Dataset to false labels as a targeted/manipulative attack (by a malevolent labeller) in the UFP, assuming that the user-labels were linked to distinct identities. The ambient data was gathered from a smart environment human activity recognition from (Continuous Ambient Sensors Dataset, CASA) with fully labeled connections.

4.PROPOSED SYSTEM

In order to identify the bwdos_sinkhole_attack attack in WSN, this section proposes the Time-varying Snapshot-based Neighbour-controlled Traffic-centric (TSNT) technique. With its low-cost, resource-constrained sensor nodes, WSNs are vulnerable to compromised nodes sending out fraudulent routing updates that break connectivity. The base station's implementation of the TSNT algorithm continuously monitors network activity and keeps track of the sensor nodes that are visited by transmitted packets, a list that changes over time. Through the use of neighbor-controlled validation and snapshot-based analysis, TSNT is able to identify abnormalities in traffic patterns that may be signs of bwdos sinkhole attacks. In order to improve service quality and secure data transmission in WSNs, the algorithm offers a reliable approach for early identification and mitigation of the attack by concentrating on the temporal evolution of network states and traffic-centric behavior.

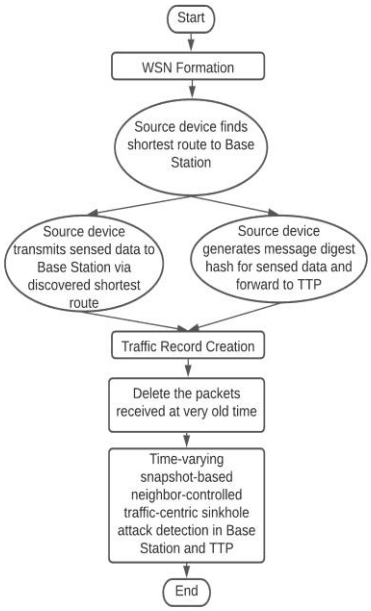

Fig. 2: Block diagram

5. Experimental Results & Discussions:

The system offers an examination of the suggested TSNT algorithm's efficacy in this section. The parameters list is presented in Table I. About 40% of the devices that were used in this simulation process were found to be malfunctioning.

Parameters	Values
Area	(900 x 600) m
No. of Devices	100
Nodes Initial Energy	100 J
Receiving Power (Er)	0.3 J
Transmission Power (Et)	0.6 J
Radio propagation range	100 m
Algorithm	TSNT
Time Threshold (TT)	2 minutes
Malicious Devices	40 %

Table I. Performance Parameters

The efficacy of the suggested TSNT and earlier algorithms is assessed in accordance with the following metrics:

1. The proportion of malicious devices detected

2. The false positive rate, or misdetection rate, of standard equipment

3. The proportion of bwdos sinkhole attack attacks that were found

Based on the aforementioned evaluation criteria, compare the TSNT method with other efforts that have been done on malicious device identification, such as Paramasiva et al., Taheri et al., and Khan et al.'s ECM-GT algorithm. The detection rate of malicious devices is displayed in Table II.

Malicious devices (%)	Paramasiva et al	Taheri et al	ECM-GT	TSNT
10	75	90	91	100
20	73	82	85	96
30	70	78	80	92
40	65	75	76	89

Table II. The detection rate of malicious devices

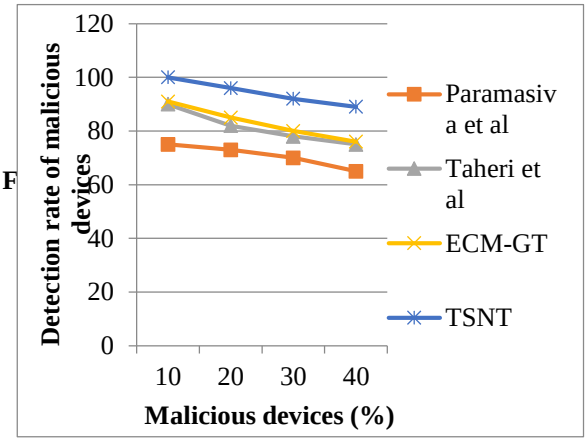

Fig. 3 shows a comparison graph of malicious devices detection rate.

The percentage of infected devices varies from 10% to 40% in Figure 3. The results clarify that, in contrast to the techniques in [36], the TSNT algorithm proved effective in identifying rogue devices. Figure 3 shows that the discovery rate shows a declining trend as the percentage of malicious devices increases. The discovery rate is significantly higher with the optimal scale than with the other three techniques.

Malicious devices (%)	Paramasiva et al	Taheri et al	ECM-GT	TSNT
10	5	3	2	0
20	7	5	3	0
30	14	10	9	5
40	23	11	10	7

Table III shows the Misdetection rate of normal devices (False Positive Rate).

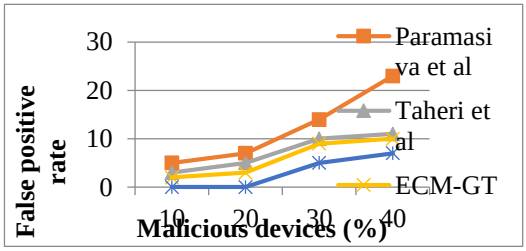

Fig. 4: False positive rate

When compared to the other three methods, Fig. 4 demonstrates that the TSNT algorithm's misdetection rate of typical devices is excessively low. Thus, it is clear from Fig. 4's false positive rate changes that the TSNT algorithm performs better than the other three.

Additionally, Table IV displays the percentage of bwdos sinkhole assaults that were detected.

Malicious devices (%)	Paramasiva et al	ECM-GT	TSNT
10	96	98	100
20	90	92	96
30	86	88	93
40	80	82	87
50	70	78	83

Table IV. Percentage of bwdos_sinkhole_attack attacks detected

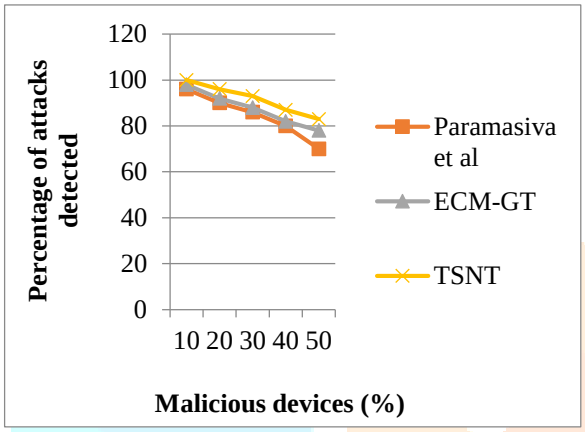

Fig. 5: Percentage of bwdos_sinkhole_attack attacks detected

As the number of hostile devices increases, Fig. 5 illustrates that the number of attacks detected decreases. The TSNT algorithm can identify overall attacks in a network when the percentage of hostile devices is lower. However, when half of the network devices are malicious, the percentage of attacks that are found decreases.

6. Conclusion:

The WSNs are useful for data collection in a variety of scenarios. However, because WSN is loosely implemented, attackers may carry out a variety of assaults. The bwdos sinkhole attack is one of the possible assaults that generates all traffic traveling through a particular device. In this work, time-varying snapshot-based bwdos_sinkhole_attack attack detection algorithm in WSN that is neighbor-controlled and traffic-centric (TSNT) to improve QoS. The base station tracks traffic using the TSNT algorithm and maintains a record of the sensor device the packet has passed through over time. Using a snapshot of the WSN collected at different times, the availability of the bwdos_sinkhole_attack was determined from this record. In the WSN network, a trustworthy third party also operates concurrently. Using data reliability confirmation based on the message-digest hash, it assists the base station in identifying the bwdos_sinkhole_attack attack. In comparison to other current algorithms, the experimental result showed that the TSNT algorithm identifies bwdos_sinkhole_attack successfully.

7. References

[1] Artificial bee colony based bwdos_sinkhole_attack detection in wireless sensor networks, Nithiyanandam N, Latha P. Humanized Computing and Ambient Intelligence Journal, July 18, 2019, 18–4.

[2] Singh A, Singh T. Review of bwdos_sinkhole_attack attack detection and prevention in the network. International Journal of Computing and Technology. Nov. 29, 2016; 5(2): 289–92.

[3] Keerthana G, Padmavathi G. Enhanced particle swarm optimization technique for detecting bwdos sinkhole attack in wireless sensor network. 2016 Mar 1;10(3):41–54; International Journal of Security and Its Applications.

[4] Attacks in Wireless Sensing using Bwdos Sinkhole Attacks by Tandon K. Research Journal of Computer and Informa. 2016 Aug;4(8):4-7.

[5] Al-Ahmadi SA, Babaeer HA. Efficient and Secure Data Transmission and Bwdos_sinkhole_attack Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking. IEEE Access, May 14, 2020