Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 5243- 5250

Research Article

A Novel Framework for Prevention of Black hole in Wireless Sensor Networks using Deep Belief Network (DBN)

Mrs. S. Gayathri[1], Mr. A. Senthilkumar[2]

Abstract

Wireless Sensor Networks are playing essential role across the world with its features and different kinds of development stages. Many researchers are contributing to build the WSN and extract its features. Intruders are involving in between the WSN signals and modify are reconstruct the entire network or framework. In past decades, Viruses and Trojans are the threats for the End user and anti-virus software are sufficient to face these threats. But now a days, passive and active attacks are occurring while transmission of network packages. Even though different kinds of threats in a WSN framework, we are contributing blackhole attack prevention mechanism using Deep Belief Network (DBN). DBN is the deep learning module and we are able to construct more number of hidden layers. We extracted the probability of black hole parameters and trained with original values for getting optimum results.

Keywords: WSN, Deep Belief Network (DBN), black hole attack

1 INTRODUCTION

Blackhole attack is an interruption, when an intermediary captures and re-programs a set of nodes in the network to block or drop the packets and generates false messages instead of forwarding the correct or true information in wireless sensor network through the base station. In routing path, the routing security methods and techniques works based on the blockage of data and the time of communication [8]. The attention of scientific and industrial domains is developed significantly by the Wireless Sensor Networks from the last decades of time. The term sensor field refers to a requisite number of sensor nodes scattered over by a WNS (Sabbir and Hassan, 2013; Sanjeev and Poonam, 2014). Node routing attackers consists of and that provide an environmental of separated attack with respect to the malicious nodes [6]. The Blackhole is a kind of Denial of Service (DoS) attack and is very difficult to detect and defend that are prone to various attacks by the Wireless Sensor Networks.

As a result, any information which enters the blackhole region is captured and not be able to reach the destination that causes high end-to-end delay and with low throughput. Previously little amount of Work is already done for both the detection and prevention methods of the blackhole

[1]Department of Computer Science Research Scholar Bharathiar university Email : gayavel82@gmail.com
[2]Department of Computer Science Arignar Anna Govt. Arts College Namakkal Email: senthilkumarmca76@gmail.com

attack in the WSN making its both the methods very crucial and essential as per the performance of the network is concerned. Initially the attack is measured on the parameters of the network followed by the proposal of a novel technique for both the methods of detection and prevention of Blackhole attack in Wireless Sensor Network.

The most important aspects and applications of Wireless Sensor Network (WSN) include the environmental monitoring, personal healthcare, enemy monitoring, etc. Often sometimes the most sensitive information is transferred and communicated to the destination node through an insecure medium. So by the Denial-of-Service (DoS) attacks, thus the WSN can be easily attacked. By these the data loss along with large energy expenditure takes place. Further, securing of the links is important in designing a sensor network. Blackhole attack is also DoS in nature.

1.1 MACHINE LEARNING IN WIRELESS SENSOR NETWORKS: ALGORITHMS, STRATEGIES, AND APPLICATIONS

Over the period of time the wireless sensor networks (WSNs) dynamically monitors the environment that changes rapidly. This change of behaviour namely dynamic is neither caused by the factors of external or by the initiated system designers themselves. To have an idea and accept to such conditions, to eliminate the needs for unnecessary redesign, the machine learning techniques with the sensory networks are often accepted or adopted. To prolong the lifespan of the network, the machine learning maximizes the resource utilization and inspires many practical solutions. In this paper, we present and a literature of extensive review over the time of 2002-2013 of machine learning methods that were used for addressing the common issues in Wireless Sensor Networks. The merits and demerits of each proposed algorithms are against the evaluation of corresponding problem. To aid WSN designers are provided with comparative guides for developing solutions for their specific application challenges using suitable Machine Learning.

1.2 A REVIEW OF ML SOLUTIONS TO DENIAL-OF -SERVICES ATTACKS IN WIRELESS SENSOR NETWORKS.

In various fields of remote data collection, the wireless sensor networks are used, such as environmental habitat monitoring, military applications, smart homes, traffic control, and health monitoring etc. The WSN are vulnerable to different or various types of attacks because they play a vital role in different domains and the sensors that are constructed by the resources. The Denial-of Service (DoS) attack is one of the main attack types that are threaten in WSNs. The various or different layers of network architecture can be carried out by DoS. In this paper the DoS attacks is reviewed at each layer of TCP/IP protocol stack. Besides that, we concentrate on the other network layers attacks due to more diverse than other attacks of Layer. A number of studies are reviewed for proposing machine learning solutions for pertaining to network layer DoS attacks in WSNs.

II LITERATURE REVIEW

Soni Rani et al. (2016) have reported that wireless sensor network has a numerous form of applications in various fields of experiments such as military, health and environmental areas. This is due to withstand of hash environmental conditions and ease of use conditions. They have also further discussed that security issues are of main that are to be concerned and networks are self-administrated in which that the nodes are to be self-organized and to have a reliable communication between them.They have discussed and expressed that the blackhole attack is

one of the very common attacks due to its stop communication from the various source of destination. They had further determined that there are numerous measures to detect and prevent the blackhole attack in networks.

They have done an experimental result on various algorithms to detect the blackhole attack. By demonstrating two specialized algorithms such as soft computing algorithms and AODV routing algorithms have done a research.

Sareen Karapoola et al. (2020) has discussed and concentrated on volumetric Distributed Denial of Service (DDoS) that are most important for the data technology-based organizations. As a victim these attacks results in revenue losses in terms of resource wastage and service of unavailability. As well as the Internet Service Provider (ISPs) along with the path of attack is demonstrated.This paper also presents or explains a detail hardware test-bed platform consisting of 30 routers on which the service of networks as a Net-police has to be implemented and a study on feasibility field.As an Experimental result reveals that the Net-Police performs better than the state-of-the-art that are traceback and cloud-based solutions in terms of the bandwidth ISP and the legitimate client's victim availability.

Baviskar et al. (2014) have concentrated and discussed that the Wireless Sensor Network consists of various nodes that can be communicated with each other by the use of Wireless Sensor Networks node is a static and it is said to be remained fixed in their position of general conception.A dominant manner for a long period of time has been deployed. They have also discussed that many researches have been mostly focused on WSN sensor nodes of energy consumption.It mainly focused and concentrated that in WSN the security is a critical issue because of the inherent limitations. Due to the computational capacity and usage of power, the blackhole attacks are one of the challenging attacks in the Security of WSN.

A set of nodes in the network is to block/ drop due to blackhole attacks when an adversary captures and re-programs a set of nodes and also, they receive and generate them towards the base station instead of forwarding them. Any data that enters the region of blackhole is captured. They have also reported that the blackholes are capable of effective and undermining network by the network partitioning. In such way the vital information doesn't reach the base stations. To overcome the blackhole attack in the networks, various techniques have been proposed on the secret sharing and multipath routing. It has been demonstrated that these techniques are not more effective, they may even end up by making more effective the blackhole attacks. It is deployed that the use of multiple base stations in network counter has the impact of data transmission of blackhole attacks. They have done an experimental result with the help of java simulator and the compare of performance with and without multiple base station to prevent the blackhole attacks.

Ankit Kumar et al. (2021) has discussed that the vehicular ad hoc networks (VANETs) which has gained a significant value in the domain research of intelligent transportation System (ITS). They have also provided a safety and security for both the drivers and passengers.VANETS are mostly differing in many terms of characteristics and the architecture of the system that is proposed. In these networks, any node can be functioned as a router for other nodes. Any network and a node connected to any network many inject the routing table by affecting the operations and tables of the networks.They have discussed as an experimental result that a secure AODV protocol of routing overcomes this issue and is used for developing the blackhole detection.

III IMPLEMENTATION

During the transmission, the malicious are keenly watching all the packets and give the fake or wrong routing information to sender and drop the packets. So we implemented a novel

framework using Deep Belief Network to identify the malicious and identify the originality of protocol structure. It is pre –trained by greedy methods with top-down priority approach and depending on the weights. DBN is working on the layer by layer approach with the stack of RBM (Restricted Boltzmann machine) algorithm. In the RBM stack, a layer is cable of communicating with previous layer and subsequent layer. In the join distribution between vector and hidden layer are calculated as

$$P(x, h^1, \ldots, h^l) = \left(\prod_{k=0}^{l-2} P(h^k | h^{k+1}) \right) P(h^{l-1}, h^l)$$

X=h_0, $P(h^k \mid h^{k+1})$ –

Conditional_Distribution
Level K = $P(h^{l-1}, h^l)$ – Visible and hidden_Joint_Distribution

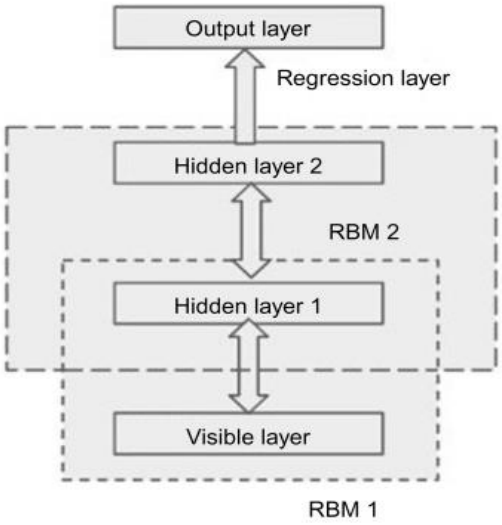

Figure 3.1 Architecture of DBM with 2 RBM

Deep neural network is used to solve two kinds of problem. They are directedproblem and Inverse problem. Directproblem is to paraphrase the cognitivefunctions of human mind system. Inverse problem is to simulate theapplications of engineering basedsystems with biological structure.This network is constructed by fewlayers. Each layer is made of nodes. The computations are performed inthis node with the construction ofneuron in human brain. A node ismixed with coefficients or weights ofthe relevant information.

d	Time	Is_CH	Who CH	Dist_To_CH	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	Dist_CH_To_BS	Consumed energy	Attack type
106079	303	1	106079	0	0	75	1	0	0	0	1350	7	108.3	1.64	Grayhole
107033	353	1	107033	0	0	71	1	0	0	0	1349	9	162.6	2.033	Grayhole
115021	753	1	115021	0	0	59	1	0	0	0	1298	0	0	0.007	Blackhole
117044	853	1	117044	0	0	54	54	0	0	0	0	0	0	0.007	Scheduling
103043	153	1	103043	0	0	47	1	0	0	0	1269	14	145.1	1.88	Grayhole
105005	253	1	105005	0	0	47	1	0	0	0	1170	7	137.6	0.921	Grayhole
110024	503	1	110024	0	0	35	1	0	0	0	1200	15	113.3	2.058	Grayhole
101041	53	1	101041	0	0	34	1	0	0	0	1258	0	0	0.002	Blackhole
102040	103	1	102040	0	0	31	1	0	0	0	1240	0	0	0.007	Blackhole
201061	1003	1	201061	0	0	31	1	0	0	0	1240	0	0	0.007	Blackhole
118058	903	1	118058	0	0	27	27	0	0	0	0	0	0	0.007	Scheduling
103003	153	1	103003	0	0	22	1	0	0	0	1166	29	85.2	2.07	Grayhole
111050	553	0	111093	15.17	1	0	0	1	10	22	0	0	0	0.042	Normal

Table 3.1 A Dataset for Intrusion Detection Systems in Wireless Sensor Networks

	Normal	Flooding	Scheduling	Grayhole	Blackhole
Normal	135488	358	40	160	20
Flooding	0	1331	0	0	0
Scheduling	32	0	2629	6	18
Grayhole	31	0	11	5400	429
Blackhole	0	0	7	2647	1384

Table 3.2 One – hidden layer (Confusion Matrix)

In Mobile Adhoc Network (MANET), Blackhole [8] is an active attack and it can process with RREQ message (Route Request). Malicious node is intruding and posts the fake copy of RREP (Request Reply). So the transmission will be happened with packet lost. We analyzed following parameters for extracting the features to overcome the black hole attack.

Parameters	**Description**
Protocol	AODV (Ad-hoc On-demand Distance Vector) Protocol
Channel Mode	Wireless Sensor
Time	120 sec
Traffic in WSN	Cooperative Balancing Routing
Packet	780
Nodes	80
Data speed	0.2 mbps

QOS	Packet delivery ratio, Delay, Overhead

Table 3.3 Parameters of Black-Hole evaluation

IV RESULT AND DISCUSSION

As we discussed in the section 3.1 and 3.2, first and foremost to suppose identify the original parameter metrics and measure the deviations from the current routing path if block hole will appear. The following steps depicts the way of processing our framework

Step 1: Malicious or Intruder identification;
Step 2: Malicious initialization; we suppose to use Boolean as true or false
Step 3: Black hole demonstration
(black hole (parameters == true)
Malicious = true
Step 4: Reconstruct Request and Reply
Step 5: Modify the routing path
Step 6: Redo Step 3 to Step 5 until the packets will be delivered
Step 7: Analyze the accuracy

Performance Analysis

No.Nodes	Packet Delivery Ratio	ABC Throughput	Proposed Throughput
5	97.04	1428.4288	1525.4688
10	96.29	1417.3888	1513.6788
15	94.9	1396.928	1491.828
20	95.94	1412.2368	1508.1768
25	98.6	1451.392	1549.992
30	94.31	1388.2432	1482.5532
35	96.8	1424.896	1521.696
40	93.94	1382.7968	1476.7368
45	94.44	1390.1568	1484.5968
50	96.93	1426.8096	1523.7396

Table 4.1 Performance analysis with ABC and DBN

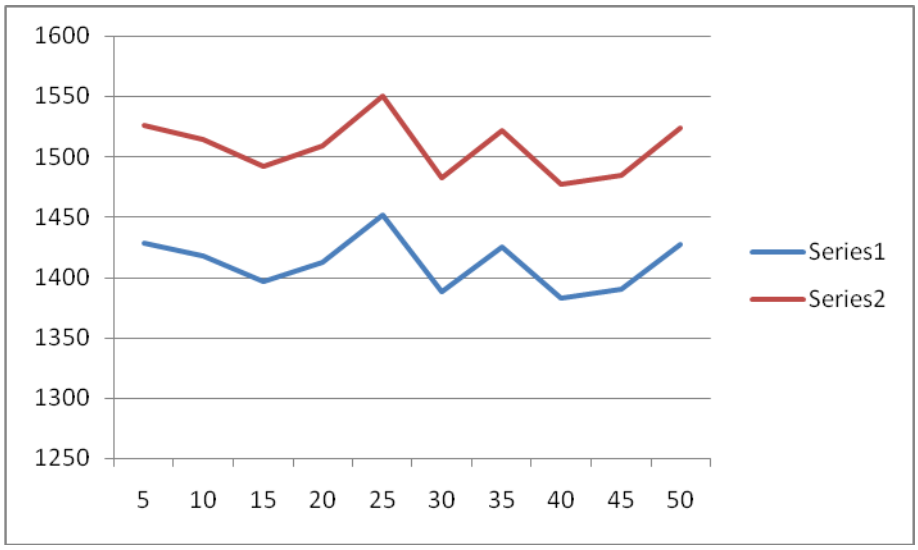

Figure 4.1 Comparison Chart

We analyzed throughput which is calculated by packet size (Estimated time – arrived time) * 0.008. Artificial Bee colony algorithms [7] with DBN algorithm have been processed and simulation results are showing the difference between them with maximum of 50 nodes.

V CONCLUSION

Today's world is function with WSN signals and data transmission. Even though WSN is the ancient concept of Information Technology but redefinition or re-configuration are essential for the researchers and society. We narrated in Chapter – I and II, significance of WSN and impacts of black hole attack. Hence we discussed with existing ABC algorithm and Deep belief network. Based on the simulation results, it shows comparatively high throughput. Trustworthy optimization, Intruder avoidance and PDR with high ratio are major parameters to define the best Wireless Sensor Network. In this paper, we have contributed black hole attack avoidance with deep learning concepts with reasonable accuracy.

REFERENCE

1. Soni Rani, C.S., 2016. A Survey of Various Algorithms to Detect Black Hole Attack in Wireless Sensor Network.
2. Baviskar BR, Patil VN. Black hole attacks mitigation and prevention in wireless sensor network. International Journal of Innovative Research in Advanced Engineering (IJIRAE). 2014 May;1(4):167-9.
3. Baviskar, B. R., and V. N. Patil. "Black hole attacks mitigation and prevention in wireless sensor network." *International Journal of Innovative Research in Advanced Engineering (IJIRAE)* 1, no. 4 (2014): 167-169.
4. Kumar A, Varadarajan V, Kumar A, Dadheech P, Choudhary SS, Kumar VA, Panigrahi BK, Veluvolu KC. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. Microprocessors and Microsystems. 2021 Feb 1;80:103352.
5. Elmahdi E, Yoo SM, Sharshembiev K. Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. Journal of Information Security and Applications. 2020 Apr 1;51:102425.

6. Karapoola S, Vairam PK, Raman S, Kamakoti V. Net-Police: A network patrolling service for effective mitigation of volumetric DDoS attacks. Computer Communications. 2020 Jan 15;150:438-54.
7. V. Keerthika, Dr. N. Malarvizhi,"Enhanced AODV Protocol to Secure Routing in MANET with Optimization Techniques", International Journal of Engineering & Technology, 7 (2.19) (2018) 75-79
8. Md Ibrahim Talukdar ,Rosilah Hassan ,Md Sharif Hossen ,**1**Khaleel Ahmad , Faizan Qamar ,and Amjed Sid Ahmed,"Performance Improvements of AODV by Black Hole AttackDetection Using IDS and Digital Signature", Hindawi- Wireless Communications and Mobile Computing, Volume 2021, Article ID 6693316,