Intrusion Detection Based on Neural Networks in IoT

Chaima BENSAID
Computer Science department
Khemis Meliana University, ALGERIA
chaima.bensaid@univ-dbkm.dz

Abstract— **Artificial neural networks (ANNs) are biologically inspired computer networks used for a wide variety of problems, based on supervised learning and comprising three layers: input, hidden and output. The Internet of Things or IoT is a set of objects, sensors, and other elements connected to an Internet or other networks, these nodes make it possible to collect and exchange data. The nature of the nodes exposes IoT to many types of attacks. In particular, the Blackhole attack. This attack is one of the active and dangerous attacks in the network layer. Therefore, the aim of this paper is to propose and study an efficient approach to detect and suppress the Blackhole attack in the IoT in the environment of the AODV routing protocol using an unsupervised learning mechanism which is a neural network. The proposal is implemented and simulated under the NS2 network simulator, the simulation results show the efficiency of the proposed system and the detection speed of the malicious node in terms of lost packets and end-to-end delay.**

Keywords—IoT, AODV ,NS2, ANN

I. INTRODUCTION

The IoT is one of the recent technologies that enable important communication is possible between vehicles, sensors, and objects. Recently, with the improvement of wireless networks, IoT is used to collect and transfer data and information in different environments.

AODV (Ad hoc On Demand Distance Vector) is a reactive routing protocol for wireless networks. The AODV routing protocol uses three different control packets to establish and repair routes. Several types of attack can break this protocol, e.g. BlackHole Attack, Sybil Attack, sinkhole Attack, etc.The blackhole attack is a DoS attack that is focused on making the resources not able to be used. this attack is an attack whose goal is to make a service unavailable, this attack acts as a hole that attracts all data packets to pass through it. Blackhole attack is an active attack launched in a wireless network in order to obtain traffic routed to a destination, by announcing false routing information. This attack constitutes a serious threat to the normal operation of the wireless network.

Our proposal introduced a new ANN-based unsupervised learning concept to detect malicious nodes in the AODV routing protocol in the IoT environment. Our proposal minimizes the packet loss rate and does not use cryptographic methods or special packets. Our method has been simulated with different parameters and shows very good performance, maximum packet delivery rate and fewer lost packets against AODV in case of attacks.

Our paper is structured as follows: In section II we introduced the AODV routing protocol and the mechanism of the blackhole attack. And in section III we presented related work. The proposed contribution and the experimental simulation with performance analysis are detailed in section IV. Section V contains our conclusion of our research.

THE AODV ROUTING PROTOCOL

The AODV routing protocol Routing is an algorithm for routing information to the right destination. The problem of routing is to determine the optimal routes for routing packets in a mobile network [1]. AODV is suitable for networks with highly dynamic topologies and is based on distance vector routing.

AODV uses three types of control packet:

1. RREQ: a message broadcast by a node wishing to send data to a destination [2].
2. RREP: once the destination has received the RREQ, it replies with an RREP as an acknowledgement, using the reverse path of the RREQ [2].
3. RRER: message sent by a node when it detects that the link with its neighbor is broken (invalid route) [3].

When a node is looking for a route to a destination, it broadcasts an RREQ route request. Neighboring nodes receiving this packet rebroadcast the packet until they reach a node with recent routing information to the destination it is looking for, or the destination itself. If the source has received the RREP, it can send data packets to the destination [4].

Several types of routing attack have been developed, including the Blackhole attack, this attack is an active attack that affects the performance of the AODV protocol. The malicious node easily hijacks the routing process. In this attack, the attacking node detects an active route if it receives an RREQ packet, In this case, the malicious node directly sends an RREP packet in which: the destination address is replaced by the forged destination address, and setting the sequence number a very high value and the hop count is replaced by a low value. The sending node uses the new information received in the forged RREP packet to update its routing table with the new information. As a result, the source node uses the forged route to send the data that will be deleted by the malicious node. [6].

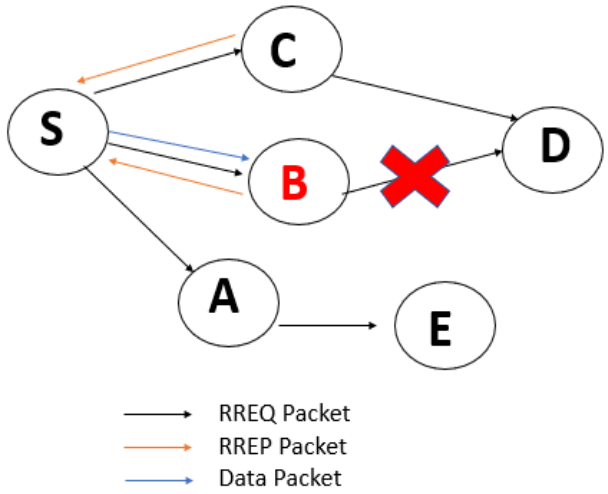

Figure 1 1 Routing discovery in AODV under DOS attack

II. RELATED WORKS

In this part, we present the works related to the DoS black hole attack problem. Which has been studied in different research studies.

The method proposed by [5] uses sequence number-based detection: the source node compares the sequence number received in the RREP with a threshold value [6]. If the sequence number received in the RREP is greater than the threshold, the RREP is suspected of being sent by a malicious party. This method uses a new packet called ALARM, which is sent to neighbors containing the blacklist. The comparison with the threshold at each time interval and the generation of ALARM packets overloads the network, increasing the end-to-end delay.

The authors of [8] have proposed an efficient method. The method is based on two steps the collection and the comparison stages. The first step involves the collection and pre-processing of RREP packets. The second step processes the sequence numbers of the RREP and discards the packets with the highest sequence number if the difference is very large. The node sending the RREP is announced as a blackhole node. And the source node alert neighbors with a packet containing the attacker's address. Each node must maintain a blacklist.

In the proposal of [9], they proposed a method based on Elliptic Curve Cryptography (ECC). Packets are encoded in ECC using a public key with a secure proxy that generates an encrypted packet. In effect, Initially, the source node generates another private key t from the generated public key. It codes the packet with the private key and publishes the public key.

In [10], the authors proposed a secure version of the AODV protocol for detecting DoS attacks. Using two new control packet,When the destination receives the new CHECKVRF control packet, it responds with the new FINALREPLY control packet to ensure that the route is dummy. The main advantages of this system are, of course, multiple routing and disproportionate energy consumption.

In [11], the authors proposed an algorithm based on setting a security bit in the RREP packet. This model assumes that the attacking node has no concerns about this validity. The source uses this path and sends its data packets if the security bit is always set.

In [12], a new feature is introduced to find nodes that refuse service as well as nodes that behave abnormally. The mechanism uses two steps, namely cache information and the hash tree, to verify these caches without disclosing the sequestration of the verified nodes.

The authors of [13] proposed a secure communication model using homomorphic encryption, in which they extended the protocol used to make data transmission secure and usefulby using a homomorphic encryption method.

In [14] and [15], the authors proposed a secure version of the AODV routing protocol (S-AODV) based on ANN and SVM to detect blackhole attacks. he authors showed that the intrusion detection rate improved by 95% in the network.

III. SYSTEM PROPOSED AND RECOMMANDATIONS

The Internet of Things (IoT) integrates nodes in order to connect to the Internet or another type of network in order to exchange and share data with them. But it is very vulnerable to DOS Blackhole attacks. In our work, we have developed a security mechanism based mainly on detection. For this, we have proposed a new protocol named AODV-BR, during the link discovery phase, a secured path is discovered so as to settle on one as the main path for data packets transmitted to the destination node. In addition, in AODV-BR, to ensure efficient communication between nodes, each node uses the IEEE 802.11p standard for transmission channel access.

In the proposed AODV-BR protocol, each node updates its list of direct neighbors. Next, the source node checks its routing

table for a valid route. If the route is available, the source sends the data packets directly with the found route, otherwise it restarts the discovery phase by broadcasting a RREQ control packet to the direct neighbors until it reaches the destination. The destination node responds with an RREP message using the reverse route chosen according to well-defined criteria '.

A mathematical machine learning model is used with the ANN model to detect attacks. The main role of the ANN is to calculate the trust value of the destination to identify malicious nodes.

The proposed AODV-BR model uses three different features x1, x2 and x3. These features are the inputs to the ANN model. The features used as inputs to the ANN are extracted from a trace (obtained by simulating our model using NS2).In the following, we will describe the necessary steps for the operation of our algorithm:

1. we used the following notation:

Table 1 Notations used

Variable	Description
Hop_Count	the number of hops between the destination X and the source sending the RREQ
N_RREP_x	the number of RREPs sent by node the destination X
Avg_RREP	the average of RREP packets sent in the network
N-Seq-SRC	source sequence number
N-Seq-DST	Destination sequence number

2. The general idea is that the malicious node uses a hop count = 1, a high sequence value in the sent RREP packets to lure the packets to pass through it and also it sends the maximum number of RREPs to destroy the service. if a source node receives a RREP from the destination node X, it will use the following algorithm to choose the value of **x1, x2 and x3**

The values of x1, x2 and x3 are chosen as follows:

Algorithm: feature selection values and detection algorithm

Begin
1.If Hop_Count ==1. X1= -1
2. Else X1=1
3.If N_RREP_X > Moy1 X2= -1
4. Else X2=1
5.If N-Seq-DST - N-Seq-SRC > 5000 X3= -1
6. Else X3=1
7. ANN structure
8. Terminate the process
End

The values of x1,x2,x3 are the inputs to ANN,The following diagram represents our architecture:

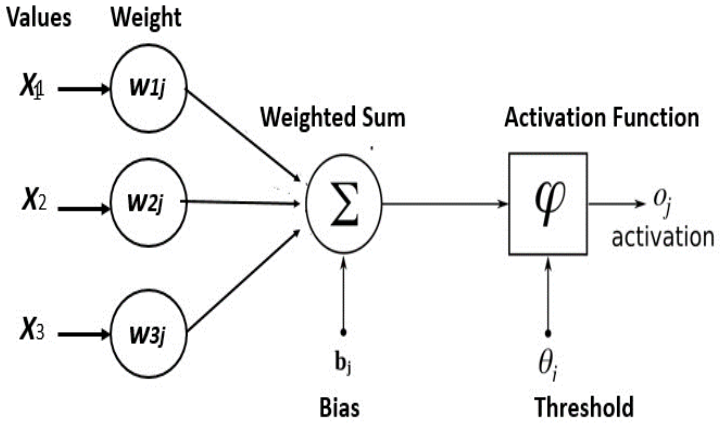

Figure 2 Routing discovery in AODV under DoS attack.

A linear activation function is used in the hidden layers so that all neurons between x1,x2,x3 are active at the same time., The inputs are represented by$XX = \{x_1, x_2, x_3\}$when $w_{1j}+w_{2j}+w_{3j}=1$ and the sum of the weighting function as $\sum_{k=0}^{3} x$ k w_{kj}
The output layer indicates the model output which is the destination confidence value that is in the interval (-1,1) since the hyperbolic or tanh function is used to activate the output node and is then assigned to the attack or not-attack class. The hyperbolic or tanh function is an extension of the logistic sigmoid; the difference is that the output here extends between -1 and +1. The hyperbolic or tanh function is triggered according to the value of the neuron output. The sign function generates 1 or 0 depending on whether or not the neuron output is greater than zero.

For exemple: If ∑ wixi> 0 Then final output "H" = 1 (not-attack) Else, final output "H" = 0 (attack

The parameters of our simulation model are shown in Table 2.

Table 2 SIMULATION PARAMATERS

Parameters	Value
simulation area (m × m)	1000 x 500
Number of nodes	10, 15,20, 30, 40
Number of communicating nodes	5, 8, 10, 15, 20
Simulation time (s)	180 s
Routing Protocol	AODV
Number of malicious nodes	3
Maximum speed (m/s)	50 m/s
Propagation Model	Nakagami
PHY layer	IEEE 802.11p
MAC layer	IEEE 802.11p
CBR packet size is	1024 bytes
CBR packet rate	100kbp

The well-known metrics to evaluate routing protocol is used in our study [16]:

- Packet Delivery Ratio (PDR): This rate represents the percentage of packets received at the correct destination in the network.
- End-to-end latency (Delay): This is the average time taken to deliver a data packet from source to destination,
- Lost packets: The rate of packets lost due to broken links or malicious nodes.

To prove the effectiveness of our proposal, we used the NS2 version 2.35 network simulator under LINUX and simulated three protocols:

1. AODV without any attack
2. AODVBLACK : AODV with 3 malicious nodes
3. AODV-BR ; our proposal protocol

- **Impact of Dropped packet.**

Table 3 Dropped packet vs number of nodes

NB-nodes	10	15	20	30	40
AODV	23	61	127	216	113
AODVBLACk	1376	3576	4684	6740	7290
AODV-BR	28	139	69	539	260

Table 3 and Figure 2 present the lost packets for the tree protocols AODV, AODV under attack, and AODV-BR. From a first view, the rate of dropped packets increases in all three protocols, when the number of nodes increases, so if the number of nodes increases, the malicious node intercepts a large number of packets, but our method is more efficient because we have used a fast mechanism to detect malicious nodes.

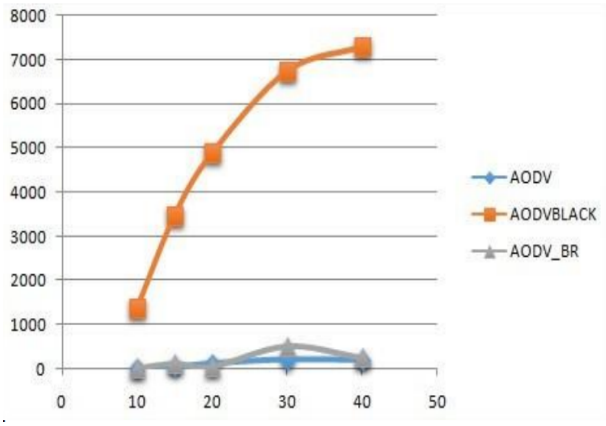

Figure 2 Dropped packet vs number of nodes

- **Impact of Dropped PDR**

Table 4 PDR vs number of nodes

NB-nodes	10	15	20	30	40
AODV	100	99,95	99,64	99,14	98,65
AODVBLACk	45,14	17,91	7,28	9,86	18,61
AODV-BR	99,99	97,78	99,69	91,63	97,86

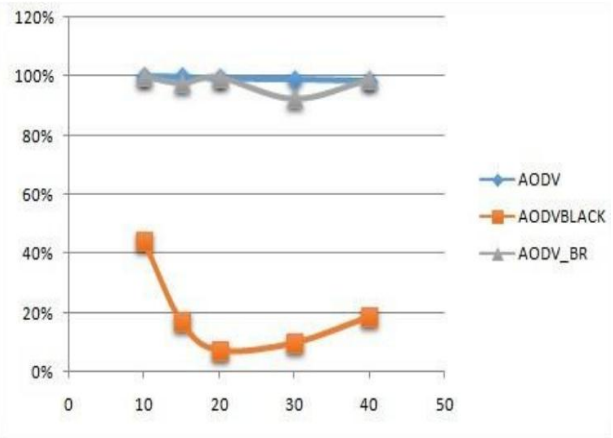

Figure 3 PDR vs number of nodes

Table 4 and Figure 3 present the Packet Delivery Ratio: evolution for the AODV, AODV under attack, and AODV-BR according to number of nodes from 10 to 40 nodes, when the number of nodes is high, the PDR of The AODV and AODV-BR register a small degradation. Subsequently, the performance of AODV under attack gradually degrades as a function of the increasing number of nodes because the malicious nodes delete the maximum of the packets sent in the network.

- **Impact of End-to-end delay**

Table 5 End-to-end delay vs. number of nodes

NB-nodes	10	15	20	30	40
AODV	0,0292	0,0049	0,0193	0,0158	0,0674
AODVBLAC	0,0028	0,0037	0,0045	0,0027	0,0259
AODV-BR	0,01	0,08	0,017	0,1445	0,1119

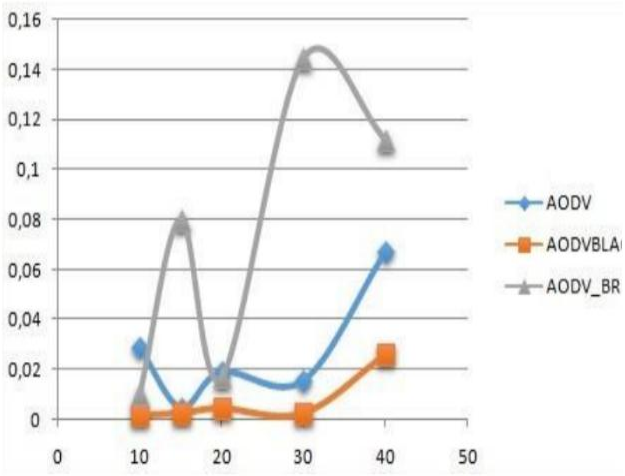

Figure 4 End-to-end delay vs. number of nodes

Table 5 and Figure 4 present the evolution of the end-to-end delay, or the AODV, AODV under attack, and AODV-BR. We note that the time elapsed by our proposal is greater than the AODV under DoS attack. This can be justified by using additional processing in our algorithm to detect and isolate malicious nodes, which increases the end-to-end delay.

IV. CONCLUSION

The paper introduced a new concept that is able to detect malicious nodes that use the DoS attack in the AODV routing protocol, Our proposal minimizes energy consumption and network overhead because it does not use cryptographic methods and no special packets. Our method has been simulated with different parameters and environment and ensure the efficiency of the proposed system and the detection speed of the malicious.

REFERENCES

[1] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, Vol. 11, pp. 38-47, Feb. 2004, DOI: 10.1109/MWC.2004.1269716.

[2] Ochola, E.O., and Eloff, M.M. (2011). A review of black hole attack on AODV routing in MANET.

[3] Raj, P. N., and Swadas, P. B. (2009). DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET. International Journal of Computer Science Issues, 7(4), 54

[4] H. Deng, W. Li, and D. P. Agarwal, "Routing Security in Wireless AdHoc Networks," in IEEE Communication Magazine, Vol. 40, pp. 70-75, Oct. 2002, DOI: 10.1109/MCOM.2002.1039859.

[5] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Jtheynal of Computer Science Issues, Vol. 2, 2009.

[6] Shurman, M. A., Yoo, S. M., and Park, S. (2004, April). Black hole attack in wireless ad hoc networks. Proceedings of theACM 42nd Southeast Conference (ACMSE 2004) (pp. 96–97)

[7] Vani, A. (2011, March). D.S.R., removal of black hole attack in ad hoc wireless networks to provide confidentiality security service. International Journal of Engineering Science and Technology, 3(3).

[8] Subash Chandra Mandhata, D. S. N. P. (2011).A counter measure to Black hole attack on AODV based Mobile Ad-Hoc Networks. International Journal of Computer Communication Technology.

[9] J. Sultana, T. Ahmed, "Elliptic Curve Cryptography Based Data Transmission against Blackhole Attack in MANET," International Journal of Electrical and Computer Engineering (IJECE), Vol. 8, No. 6, pp. 4412- 4422, Dec. 2018, DOI: 10.11591/ijece.v8i6.pp.4412-4422.

[10] Chavan, A.A.; Kurule, D.S.; Dere, P.U. Performance analysis of AODV and DSDV routing protocol in MANET and modifica- tions in AODV against black hole attack. Procedia Comput. Sci. 2016, 79, 835–844.

[11]Deshmukh, S.R.; Chatur, P.N.; Bhople, N.B. AODV-based secure routing against blackhole attack in MANET. In Proceedings of the International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Benga- luru, India, 20–21 May 2016; pp. 1960–1964

[12] Li, T.; Ma, J.; Pei, Q.; Song, H.; Shen, Y.; Sun, C. DAPV: Diagnosing Anomalies in MANETs Routing with Provenance and verification IEEE Access 2018, 7, 35302–35316.

[13] E. Elmahdi, S. Yoo, K. Sharshembiev, "Secure and reliable dataforwarding using homomorphic encryption against blackhole attacks inmobile ad hoc networks, " Journal of Information Security andApplications, Vol. 51, p. 102425, April. 2020, DOI:10.1016/j.jisa.2019.102425

[14] Basomingera, R. and Choi, Y.J., 2019, January. Route cache based SVM classifier for intrusion detection of control packet attacks in mobile ad-hoc networks. In 2019 International Conference on Information Networking (ICOIN) (pp. 31-36). IEEE.

[15] Pandey, S. and Singh, V., 2020, July. Blackhole attack detection using machine learning approach on MANET. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 797-802). IEEE.

[16] C.Bensaid and Boukli Hacene, S. (june 2016). Detection and Ignoring of Blackhole Attack in Vanets Networks , International Journal of Cloud Applications and Computing, Volume 6 • Issue 2 • April-June-2016 • ISSN: 2156-1834 • eISSN: 2156-182