Performance Analysis of Nash Algorithm to Detect the Jamming Attack in IoT Network

C.Manikandan [1], and V. Alamelumangai [2]

[1] Research scholar [2] Professor
[1, 2] Department of Electronics and Instrumentation Engineering, Annamalai University, India
E-mail: manikandan.aec@gmail.com

Abstract: *The Nash algorithm was proposed for detecting the jamming node which improves the secure data transmission between the source nodes to the sink node in industrial IoT network. Once the jamming node is detected the action performed by the normal and jamming node is detected. Then the number of successful transmission and unsuccessful transmission also detected. The performance metrics of the proposed technique are also analyzed using PDR, throughput.*

Keywords: Jamming attack, Nash algorithm, industrial IoT network

1. Introduction

One of the major challenges an Internet of Things (IoT) networks face today is security. Such a network normally consists of a large number of distributed nodes that organize themselves into a multi-hop wireless structure. Each node has one or more sensors, embedded processors and low-power radios. Typically, these nodes coordinated to perform a common task. The deployment of sensor nodes in an industrial environment makes the network vulnerable to a variety of potential attacks some of which are eavesdropping attack, corrupted node, jamming attack, collision attack, and man in the middle attack.

Jamming attacks can be described as any disorder or obstruction with the physical transmission and reception of wireless signals. This can be either intentional or unintentional. In case of intentional, attackers generated the interference frequency in the form of radio signal. In case of unintentional, collision and noise interference occurs at the receiver.

The main objective of the jamming attack is to disrupt the successful communication between the transmitter and receiver. Jamming is one such denial of service attack which prevents the network from performing its basic functions. Jamming is defined as interfering with the legitimate frequency of sensor nodes.

Wormhole threat technique gives a solution to bring out the message out of jammed area. This is done using three steps (i) Wired pair of sensors, (ii) frequency hopping and (iii) uncorrelated channel hopping. The drawbacks of these techniques are that it is complex, costly and requires synchronization.

Uncoordinated Frequency Hopping (UFH) scheme which provides jamming free communication between two nodes in the presence of jammer without shared keys. UFH scheme is used for key establishment protocol that enables the nodes to agree on a shared key which will be further used to create secret hopping sequence and communicate using coordinated frequency hopping. The drawback is that it has low throughput, it requires high storage and high processing cost.

2. Nash Algorithm

Consider an IoT system consisting of an Access Point (AP) and a set of n sensor nodes connected to the AP for communicating with one another and sharing data. The IoT devices are connected to the AP over an IEEE 802.11ah (low-power WiFi) protocol which is known to be a suitable wireless solution for resource-constraint IoT devices

Step 1: Establish a network system consisting of an AP and a set of n sensor nodes.

The first step in the proposed technique is to establish the network with n number of nodes. The nodes randomly arranged on their location as shown in Figure. 1 and sense the sensor information. Once the valid data is obtained the source node is transmit the information to the sink node.

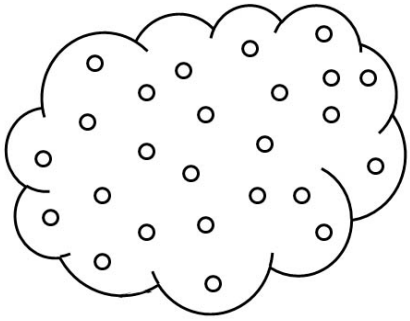

Figure. 1 A Network with n no of nodes

Step 2 Divide the network into segments.

This step divides the randomly generated network in to segments to determine the jamming attack from each segment. The Figure.2 shows that the network is divided into four segments.

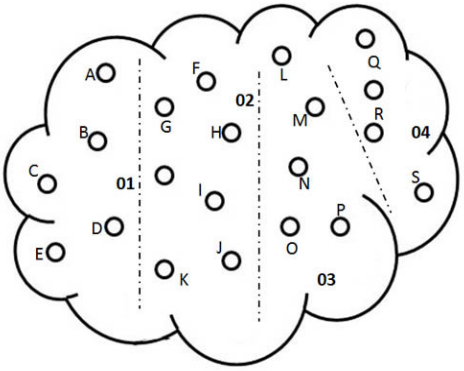

Figure.2 A Network with four segments

Step 3 Find the probability of successful transmission of nodes in each segment.

A network has n nodes in which a specific node transmitting in a given slot with probability p for its transmission to be successful, all the other nodes should not send. That combined probability is $p\ (1-p)^{N-1}$.so the probability of exactly one node successfully transmitting in N ways in a given slot is $np(1-p)^{n-1}$.

Step 4 Nash Equilibrium

Nash equilibrium is a fundamental concept in the theory of games and the most widely used method of predicting the outcome of the nodes in wireless network. A game consists of the following three elements they are, set of players (nodes), set of actions available for each nodes and payoff functions. The payoff function represents each node preference over action profile where an action profile is simply a list of action, one for each node. Find the probability of successful transmission of each node in the segment 1 and segment 2 shown in Figure.2.

Table. 1 shows that segment 1 have node A, B, C, D and E and segment2 have node F, G, H, I, J and K. $p_{(A,F)}$ gives the probability of successful transmission of data from node A to F. Similarly the probabilities for all other nodes are presented in Table 1. The obtained values in the Table 1, if any row or any column has less value as compared to other rows and columns then the corresponding node is identified as jamming node.

Table .1 Nash Equilibrium concept segment 1 and segment 2

Segment1 \ Segment2	F	G	H	I	J	K
A	$p_{(A,F)}$, $p_{(F,A)}$	$p_{(A,G)}$, $p_{(G,A)}$	$p_{(A,H)}$, $p_{(H,A)}$	$p_{(A,I)}$, $p_{(I,A)}$	$p_{(A,J)}$, $p_{(J,A)}$	$p_{(A,K)}$, $p_{(K,A)}$
B	$p_{(B,F)}$, $p_{(F,B)}$	$p_{(B,G)}$, $p_{(G,B)}$	$p_{(B,H)}$, $p_{(H,B)}$	$p_{(B,I)}$, $p_{(I,B)}$	$p_{(B,J)}$, $p_{(J,B)}$	$p_{(B,K)}$, $p_{(K,B)}$
C	$p_{(C,F)}$, $p_{(F,C)}$	$p_{(C,G)}$, $p_{(G,C)}$	$p_{(C,H)}$, $p_{(H,C)}$	$p_{(C,I)}$, $p_{(I,C)}$	$p_{(C,J)}$, $p_{(J,C)}$	$p_{(C,K)}$, $p_{(K,C)}$
D	$p_{(D,F)}$, $p_{(F,D)}$	$p_{(D,G)}$, $p_{(G,D)}$	$p_{(D,H)}$, $p_{(H,D)}$	$p_{(D,I)}$, $p_{(I,D)}$	$p_{(D,J)}$, $p_{(J,D)}$	$p_{(D,K)}$, $p_{(K,D)}$
E	$p_{(E,F)}$, $p_{(F,E)}$	$p_{(E,G)}$, $p_{(F,E)}$	$p_{(E,H)}$, $p_{(F,E)}$	$p_{(E,I)}$, $p_{(F,E)}$	$p_{(E,J)}$, $p_{(J,E)}$	$p_{(E,K)}$, $p_{(K,E)}$

Step 5 Signal-to-Interference-Plus Noise Ratios (SINR)

Let $\mathcal{D} = \{d1, d2... d_N\}$ and $\mathcal{S} = \{s1, s2.... s_M\}$ be respectively, the set of N IoT devices and the set of M subcarriers. It is assumed that the sub-carriers' bandwidth is relatively small compared to the total bandwidth of the network; the subcarriers are modeled as flat-fading Rayleigh channels between the devices and AP.

A jammer J which aims at disturbing the performance of IoT network by transmitting over specific subcarriers (tones) and thereby interfering with the communication of IoT devices and increasing their (Bit Error Rate) BER.

Considering the fact that the jamming signal and the information signal are both independently attenuated by the channel, the instantaneous Signal-to-Interference-Plus Noise Ratio (SINR) over a subcarrier s is given by:

$$\gamma_s = g_s^{AP} p_s / (N_0 + g_s^J j_s) \quad (1)$$

Where,

g_s^{AP}, g_s^J are the channel capacity over subcarrier for the AP and the jammer J.

p_s and j_s are the signal strength over subcarrier and jamming over subcarrier.

N_0 denotes the noise and it is assumed to be constant over all the subcarrier.

The jammer attempts to compromise the network performance by allocating its power over the subcarriers so as to degrade the received SINR and increase the BER. To successfully transmit the information packets over the subcarrier s, the received SINR γs must exceed a threshold τ. Therefore, the condition of having a successful transmission over subcarrier s is given by,

$$g_s^{AP} p_s / (N_0 + g_s^J j_s) \geq \tau. \quad (2)$$

Step 6 Expected payoff function

It is assumed that in a population of *size* $n = n_{AP} + n_J$ of n_{AP} players of the type AP and n_J players of the type J. Players of the same type have identical resources; however, each player may adopt a different strategy profile.

The strategy of each player at time step t is characterized by its probability distribution $f(x, t)$ or $h(x, t)$ if the player is of type AP or of type J respectively.

$f(x, t)$ and $h(x, t)$ are probabilities of allocating x resources at any given subcarrier at time t by a player. At each time step, each player of type AP faces the opponents of the opposite type and its expected payoff function is given by,

$$\Pi^i_{AP} = \frac{1}{n_J} \sum_{Z=1}^{n_J} \int_0^{P^{AP}} \int_0^{P^J} U_{AP}\,(fi(x,t), hz(x',t))\,dx\,dx' \quad (3)$$

$\forall i \in \{1, 2, \ldots, n_{AP}\}$

Similarly, at each time step, each player of type J faces the opponents of the opposite type and the its expected payoff function is given by,

$$\Pi^i_J = \frac{1}{n_{AP}} \sum_{Z=1}^{n_{AP}} \int_0^{P^{AP}} \int_0^{P^J} U_J\,(fz(x,t), hi(x',t))\,dx\,dx' \quad (4)$$

$\forall i \in \{1, 2, \ldots, n_J\}$

Where,

P^{AP} and P^J denotes the limited power budget of access point and jammer.

U_{AP} denotes the utility function of the access point.

U_J denotes the utility function of the jammer.

Expected payoff function of AP is given as the number of successful transmissions over M available subcarriers,

$$U_{AP}\,(ps, js) \;=\; 1/\,M \;\|\; \{s \;|\; \gamma s \;\geq\; \tau\} \;\| \qquad (5)$$

Where $\| \, . \, \|$ denotes cardinality of the set.

Expected payoff function of jammer is given as the number of unsuccessful transmissions over M available subcarriers,

$$U_J\,(ps, js) = 1\,/M \;\|\; \{s \;|\; \gamma s < \tau\} \;\| \qquad (6)$$

The utility functions in Equation (5) and (6) show that the payoff of each player depends on both its own power allocation strategy and that of its opponent.

From Table 1 a jamming node is detected using Nash equilibrium. Once a jamming node is detected what the action is performed by that node is calculated from the equation 4. And also the action performed by the other nodes in the segment can be calculated from the equation 3. Once the action is desired the number of successful transmission and number of unsuccessful transmission can be calculated from the equation 5 and 6.

The various steps presented for the proposed NASH algorithm are consolidated that the jamming node is identified from the value of probability of successful transmission of data from one node to other in a given network (as in Table 1) and SINR, payoff function and utility function are calculated for identified jamming node. From these calculated values it may be concluded that higher these values for AP represents good performance of the network compared these values for jamming nodes.

4. RESULTS AND DISCUSSION

To analyze the behavior of the network, Network Simulator 2.0 (NS2) software is preferred. The proposed technique has been implemented using Network Simulator 2.0 (NS2) software. The NS2 affords a simulation environment in response to the network characteristics and condition. The channel model designed in NS2 is dependent and quickly responsive to the relative speed and environment. In this work the sensor network is initially constructed with 200 numbers of nodes and each node has the inbuilt omni directional antenna to transmit and receive the data and control messages from other nodes in the network. The energy level of the inbuilt battery of each node is kept as 1000 Joules at an initial stage. Each node consumes certain amount of energy during the data transmission and reception and the energy consumption is entirely based on the distance between two nodes and the amount of data to be transmitted or received over the wireless medium. Dynamic source routing protocol is assigned in each node for finding the shortest path between nodes in network. The performance analysis is carried out in terms of network throughput, PDR and energy consumption.

Table.2 Performance evaluation and comparison of the proposed method with respect to number of jamming nodes (PDR %)

Number of jamming nodes	PDR (%)		
	Proposed technique	Wormhole threat technique	Uncoordinated Frequency Hopping (UFH) scheme
10	98	95.37	93.47

15	96	94.75	92.28
20	95	92.46	92.00
25	92	91.36	91.37

Table .3 Performance evaluation and comparison of the proposed method with respect to number of jamming nodes (Throughput)

Number of jamming nodes	Throughput (bits/sec)		
	Proposed technique	Wormhole threat technique	Uncoordinated Frequency Hopping (UFH) scheme
10	12,378	11,395	10,383
15	11,393	10,986	10,120
20	10,753	10,741	9865
25	9864	9654	9753

Table .4 Performance evaluation and comparison of the proposed method with respect to number of jamming nodes (Energy consumption)

Number of jamming nodes	Energy consumption (mJ)		
	Proposed technique	Wormhole threat technique	Uncoordinated Frequency Hopping (UFH) scheme
10	18	21	22
15	27	28	31
20	43	45	48
25	79	81	91

5. SUMMARY

The proposed technique using Nash algorithm game theory method has used to find the jamming node. The performance of the proposed methodology is analyzed in terms of throughput, PDR and energy consumption. The result shows that this technique is better than other existing techniques. The proposed technique achieves 98% PDR, 12,378 bits/sec throughputs and 18mJ Energy consumption.

REFERENCES

[1]. *Abdelhakim, L., Lightfoot, and Li,T.,, "Reliable Data Fusion in Wireless Sensor Networks under Byzantine Attacks", IEEE Military Communication Conference, Proceedings,* ***(2011)****, pp.810-815.*

[2]. *Abhisek Kumar, "A Survey Paper on Detection and Prevention of Black Hole in MANET", International Research Journal Of Mathematics Engineering, Vol.1 (2),* ***(2014),*** *pp17-27.*

[3]. *Aditya Vempaty, PriyadipRay, Pramod,K., and Varshney, "False Discovery Rate Based Distributed Detection in the Presence of Byzantines", IEEE Transactions on Aerospace and Electronic Systems, Vol. 50(3),* ***(2014),*** *pp. 1826 – 1840.*

[4]. *Aivaloglou,E and Gritzalis,S," Hybrid trust and reputation management for sensor networks". Wireless Networks, Vol.16 (5),* ***(2010),*** *pp.1493–1510.*

[5]. *Ajith Kumar S., Knut Øvsthus, Lars M. Kristensen, "An Industrial Perspective on Wireless Sensor Networks - A Survey of Requirements, Protocols and Challenges", IEEE Communications Surveys and Tutorials. Vol.16 (3),* ***(2014),*** *pp. 1391 – 1412.*

[6]. *Abdelhakim, L., Lightfoot, and Li,T.," Reliable Data Fusion in Wireless Sensor Networks under Byzantine Attacks", IEEE Military Communication Conference, Proceedings,* ***(2011),*** *pp.810-815.*

[7*]. Mpitziopoulos A; Gavalas D; Pantziou G; Konstantopoulos C; "Defending Wireless Sensor Networks from Jamming Attacks," 18th International Symposium on Personal Indoor and Mobile Radio Communications. PIMRC 2007. IEEE,* ***(2007),*** *pp.1-5,.*

[8]. *A.D.Wood and J.A.Stankovic, "Denial of service in sensor networks", Computer, 35(10),* ***(2002) ,****pp. 54-62.*