JEAS

JOURNAL OF ENGINEERING AND APPLIED SCIENCES

Journal of Engineering and Applied Sciences, Volume 18, Number 1, June 2021, 317-328

Game Theoretic Model for Jamming Attack Mitigation in Wireless Sensor Networks

Duru Chukwuemeka Clifford
Imo State University, Owerri
chukwuemekacduru@gmail.com

Abstract
Jamming attack is a form of denial of service attack that disrupts normal network operations. These attacks which are broadly categorized as constant jamming, deceptive jamming, random jamming or reactive jamming are able to send malicious signals in a network thereby reducing throughput and resulting to excessive energy consumption and power drainage on the part of wireless sensors associated with the compromised network. This work employs Game Theory Technique to model and mitigate jamming attacks in wireless sensor network. A comparative analysis was done between the developed enhanced security framework - game theory solution and optimal strategy reviewed in this work and it was observed that at maximum number of malicious nodes (16), enhanced game theory solution developed in this reduced average energy consumption by 11.6% and 27.49% when compared with game theory and optimal strategy solution respectively. The same applies to average delay where there is an improvement of 10.6% and 22% respectively while for average throughput, there is a 13.2% and 19.05% improvement.

Keyword: Constant, Deceptive, Random and Reactive Jamming, Game Theory

1. Introduction

Wireless Sensor Networks (WSN)form the underlying technology for most Internet of things deployment.These networks comprises of a horde of interconnected sensors having the ability to collect and process data from their associated environment and affect same through actuators. These sensors provide means of quantifying and reading physical phenomenon like temperature, chemical concentration, humidity and pressure (Ayaz et al. 2018). Recently, there has been an increase in the dependence on sensors by many aspects of human live even things as common as clothing with little to no disruption to comfort(Wang et al. 2015). Sensors are embedded in human bodies, our surrounding environment to measure and observe its characteristic and monitor human health and safety(Ajami & Teimouri 2015).

They are used to monitor vital signs of patients, athlete, children, premature babies, psychiatric patients, the elderly who required prolonged care and people in areas that are at a reasonable distance from health care professionals. Sensors have shown remarkable promises in timely diagnosis, response, control and treatment of diseases (Alotaibi & Federico 2017). A major threat to WSN is Denial of Service Attacks (DoS) which are attacks that maliciously deplete system resources like power, and channel availability. Since most sensors employed in WSN are highly constrained in terms of power and computational resources a DOS attack in the network would usually have a deeper effect on the overall system than it would for regular computer networks (Opeyemi, Attahiru & Gerhard 2018). The new trend is to employ Intrusion Detection System (IDS) for detecting malicious activities in a WSN (Aswathy et al. 2012) once this DOS threat is detected, a mitigation method is quickly activated.

2.0 Jamming Attack in Wireless Sensor Networks

Normal operation of sensors or nodes in an IoT deployment is disrupted by jamming. The jamming node emit electromagnetic signal to either jam the channel or keep it so busy that no node would ever find it idle to be able to transmit which usually result in DoS. Since MAC rules are always enforced, nodes are designed to sense the channel

for idleness to determine whether to start transmission or not. A jammer node does not follow these rules. Below is brief description of some of the common jamming techniques employed by adversaries (Duru et al. 2020).

1. Constant Jamming: Here the jamming node (attacker) constantly emits radio signal without following MAC rules for that particular network. This would prevent legitimate traffic sources from getting hold of the channel as they would always find it busy once they sense it. A major challenge here is high energy requirement of the constant jammer that result in quick battery exhaustion for the jammer node.
2. Deceptive jamming: For constant jamming, the jamming node continuously sends out streams of packet. This form can easily be recognized as the jamming pattern depicts unusual traffic in the network. Deceptive jamming sends regular packets with predefined intervals making the network believe that it might actually be coming from a legitimate source thereby keeping them in a receive state.
3. Random jamming: Random jamming alternates between sleep mode and jamming mode. During the jamming mode it sends out streams of packet to the network without obeying the predefined MAC rules. By alternating between sleep mode and jamming mode a random jammer can actually save its power hence the attack can last longer, since power is a major challenge for most of these devices. This technique gives the random jammer an edge over the previously discussed schemes. During jamming mode, the random jammer can either act as a constant jammer or deceptive jammer.
4. Reactive jamming: Unlike the jamming attack modes previously discussed, reactive jamming employs a strategy in such a way that it only resumes sending of packets once it discovers that there is an activity in the channel. It goes back to sleep mode once the channel is idle thereby saving lots of energy.

2.1 Related Works

As stated earlier, billions of devices interact and exchange information through a horde of sensor deployed together as a WSN. These interactions create a plethora of vulnerabilities for these devices' manipulation on a large scale. Authorization, Authentication and Privacy have been identified as critical problems in WSN(Riahi et al. 2013) and must be properly addressed for general user acceptance and trust on these systems. Recently there have been so many works and research on WSN security, below are a few works in this area alongside their shortcomings;

Potrino, Rango & Faz (2019) proposed a Distributed Mitigation Strategy against DoS attacks in Edge Computing. In their work, they applied Elliptic Curve Cryptography(ECC) on Message Queuing Telemetry Transport(MQTT) based communication with the aim of reducing data tempering and eavesdropping. They based their work on User Datagram Protocol (UDP) communication with the notion that UDP is lighter than TCP protocols generally used for MQTT protocols over fog computing. Their choice for a lighter protocol is understandable due to the computational limitation of devices used in edge computing. The message sending frequency of the lightweight nodes here is also made dynamic to compensate for the lack of congestion control of UDP communication. Their system being based on UDP instead of the usual SSL/TLS secure protocols inherits the fundamental flaws of UDP communication which includes jitter, lack of congestion/flow control and primitive form of error detection. Also, ECC significantly increases the size of the encrypted messages when compared with that of RSA and it has a complex implementation process resulting in the possibility of error introduction during implementation subsequently reducing the security of the whole algorithm.

Kajwadkar & Jain, (2018) proposed A Novel Algorithm for DoS and DDoS attack detection in Internet of Things. Their algorithm tries to detect DoS and DDoS attacks at an early time before it gets to the IoT end devices. They implemented this algorithm at the 6LoWPAN boarder router since all the packets entering the network usually pass through the boarder router. They have also categorized incoming packets as either blacklist, greylist or non blacklist packets which are usually determined by checking the header of the packets. Their approach uses two algorithm; primary check and secondary check algorithm. The primary check determines whether the incoming packet belongs to blacklist group, greylist group or non-blacklist group. The secondary check is invoked by the primary check to confirm if the payload of the stream incoming packets is bigger than the threshold payload set for the network. This check helps in determining whether there is a DoS attack or not.

The system's too much reliance on the boarder router makes the overall security architecture weak. This is because if the boarder router is compromised, the overall network fails. Also, their system involves two levels of checks to be performed by the boarder router on incoming packets before letting them through the network. These primary and secondary checks further add to the overall delay in the network. Jiang et al. (2015) proposed an efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Unfortunately, this scheme has some shortcomings as observed by (Das 2016) thus; It has shown to be insecure against privileged insider, The

registration phase for sensor nodes it employs is inefficient, Its login and authentication phase has no proper security, Modifying legitimate user password once it has been compromise during its password update phase is not as quick as expected and There is no provision for new sensor node addition once the scheme is deployed.

He, Kumar & Chilamkurti (2015)proposed a secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. In 2016 (Kumari et al. 2016) identified some security limitations in their scheme which they tried to circumvent by proposing mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. Kumari showed that He's scheme is prone to stolen verifier, password guessing and impersonation of users and smart card attacks. This scheme has inadequate security between a user and a sensor node due to lack of session key security also, there is no forward secrecy in the overall scheme. This implies that once a session is compromised by an adversary, its specific critical temporary information could be leaked. Kalra & Sood (2015) employed the Elliptic Curve Cryptographic system which is a public key encryption for authentication and security of IoT devices and the cloud servers. Although ECC is more promising in terms of memory and computational power requirement than most asymmetric algorithms, it required more memory and computational power than symmetric key cryptography. (Danger et al. 2013) have also demonstrated that some side channel attacks are possible with ECC implying that their scheme can be compromised using side channel attacks.

Shin et al. (2014) have proposed an effective authentication mechanism for ubiquitous collaboration in heterogeneous computing environment. Their scheme is a ticket based authentication system which cannot be applied to high resource constrained devices due to the large memory requirement of their scheme. Nevertheless, with respect to IoT deployments that have WSN integrated in it, their work has almost zero contribution to securing such systems. This is because network stability and device mobility were not properly addressed by them which are critical features for most WSN. Although the authors have employed AES based encryption scheme there is no proper key management system established in their work. Also, since AES is symmetric key cryptography the process of securely sharing key between the ticket manager and users (sensor nodes) is not guaranteed in their work. This key can be compromised on transit as they have relied solely on the strength of the ciphers of AES encryption scheme. They have assumed that even if an adversary gets hold of the key that it will remain unbreakable.

Jan et al. (2014) proposed a robust authentication mechanism based on AES encryption standards. Communication here is granted to the requesting device based on the availability of the requested resource at the server. Although the researchers have employed the traditional Constrained Application Protocol (CoAP) and have claimed to have added extra security features to it to enable it mitigate against more threats. Permission to use the network resources is delegated to the server and there is no key management mechanism employed for key exchange which should have been implemented since they have chosen to use symmetric key cryptography. Also, device ID and authentication key for all the associated devices is stored on this server. A malicious access to this server would probably compromise the overall system. Since the server and the IoT device use shared key resource to authenticate each other which remains a secret between them, loss of this key compromises the whole system and the two parties must agree and replace the key. This is a major setback for this scheme.

Bhattacharyya et al. (2014) proposed a Lightweight Mutual Authentication for CoAP based on the Datagram Transport Layer Security (DTLS). However, the DTLS implementation is originally specified to employ full Public Key Infrastructure (PKI) which is known not to be a resource-optimal solution for the constrained devices. But the authors have claimed they can achieve this authentication scheme via a unicast communication channel with a symmetric encryption (honestly, this feature is uncommon with Datagram Transport Layer Security Schemes - DTLS) that would reduce energy consumption features. The authors are yet to validate their claims till date as there was no detailed test of their system in the work. They have left the validation to future research.

Babar, Prasad, & Prasad (2013) designed a Game theoretic modeling of WSN jamming attack and detection mechanism. In their work they proposed a mixed strategy game formulation for the mitigation of the jamming attack once discovered. Comparing the effect of their proposed detection and mitigation mechanism with optimal jamming strategy proposed by (Li, Koutsopoulos & Poovendran 2010), it could be seen that there is a huge improvement in the network metrics. Part of the reasons for this is the carrier sensing method employed. While Li employed slotted ALOHA, Sachin D. et al employed Carrier Sense Multiple Access with Collision Detection (CSMA/CD). CSMA/CD has shown better results for wireless network when compared to most multi-access protocols (Forouzan, 2007). Although their system has shown good results, the cross layer features they employed use retransmission of

data which is not the best option for the intrusion detection system adopted. This is because, retransmission of data as a cross layer feature would require considerable channel time to be detected, analyzed and grouped as an anomaly. This makes the detection algorithm a bit slow since the size of the data to be retransmitted would normally vary according to the rules set by the network.

Li proposed An Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks (Li, Koutsopoulos & Poovendran 2010). They derived optimal attack and defense strategies as solutions to optimization problems experienced by the network and attacker. For detection purpose, they allowed the network to operate under no collision condition and a record of the nominal collision during this period is taken. It is assumed that increased collision rate signifies the presence of a jammer in their network.

Their detection algorithm is based on collision in the network which is a really poor choice as many other factors can actually cause collision in any particular network. The underlying carrier sensing method employed in their work (slotted Aloha type Random access protocol) has been shown to be inadequate (Forouzan 2007). This is because detecting collision in a wireless network is always a difficult task because of the low energy of retransmitted signals in case of an error in the channel. Also, slotted ALOHA derives its strength by ensuring that communicating nodes send packet at the beginning of their time slots but this is not always the case. Two or more stations may actually send packets at the beginning of the same time slot causing collision.

Most of the security framework proposed and implemented so far did not address the key exchange mechanism when symmetrical key cryptography is being employed. A man in the middle attack can easily get the symmetric key of the system during key exchange thereby compromising the overall network. Also a few of the proposed framework employs asymmetric key cryptography that is known to be highly resource demanding due to the key size and because these nodes need to maintain two different keys (public and private keys) for secure information exchange. Since most devices employed in IoT are constrained in terms of memory, public key cryptography is not always the best solution rather a hybrid system is recommended where the crypto keys are based on symmetric key cryptography and a suitable public key cryptosystem is employed for secure key exchange mechanism. The major challenge in symmetric key cryptography lies mainly in ensuring that the key exchange process between nodes is managed securely and cannot be compromised by man in the middle attack or side channel attack.

Secondly, a few of the researches reviewed had focused mainly on cryptanalysis attack with less attention paid to DoS and malicious exhaustion of the network resources. Those that have done a considerable work in this area have employed poor methods and made inadequate assumptions that need to be reviewed and improved. For instance, the slotted ALOHA used by Li et al as shown above is a very poor choice for wireless networks (Forouzan 2007). Also, the cross layer features employed for their detection algorithm is insufficient if early and effective detection of the jamming attack is of paramount interest (Babar, Prasad & Prasad 2013).

This work has enforced an adapted CSMA/CA on nodes in the network as against ALOHA employed by a few works reviewed in section 2.1. Also, ratio of Request to Send/Clear to Send, Network Allocation Vector and Carrier sense failure frequency are the unique cross-layer features employed in the design of the clustering algorithm for the detection of jamming activity. These cross-layer features helps in early detection hence, activation of the mitigation strategy developed in this work. The rate of false positives is also reduced by employing these cross-layer features.

3.0 Design of Game Theoretic Model for Jamming Attack Mitigation in Wireless Sensor Networks.

A game theory model was used to form strategies for the jammer node and the monitoring node (honest node). The model provides utilities and payoff for successful jamming and successful mitigation of the attack. Nash equilibrium is established whereby the jammer node has no motivation to increase its payoff (by changing jamming strategy) and the honest node has no motivation to increase its payoff (change the mitigation strategies). The Nash equilibrium is the solution to the mitigation problem since at this point, the jammer node has no motivation to continue jamming (no positive change in gain or payoff) and the honest node has no motivation to change its monitoring strategy based on the same reason. The model is designed as a two-player, non-cooperative, mixed strategy game having A as the honest node and B as the jammer node. The player set becomes {A, B}.

The strategy for the honest node A is either to monitor the channel continuously to detect jamming or monitor the channel periodically (predetermined interval) both are denoted as M_c and $M_p$respectively. Continuous monitoring demands high energy but is more likely not to miss any attack while periodic monitoring demands less energy and may miss some attacks.

The jamming node can either adopt constant, deceptive, random and reactive jamming strategies thus;

a. It can act as a constant jammer denoted by: Con_j
b. It can act as a Deceptive jammer denoted by: Dec_j
c. It can act as a Random jammer denoted by: Ran_j
d. It can act as a Reactive jammer denoted by: Rec_j

From the foregoing, the techniques set for the honest node can be denoted as M_c and M_p while that for the jammer node is denoted as Con_j, Dec_j, Ran_j, and Rec_j. The strategy set is then given as S = S1 x S2, where S1 = { M_c, M_p} for Player 1, the honest node and S2 = { Con_j, Dec_j, Ran_j, Rec_j} for player 2, jammer node. For the purpose of formulating the game model, the payoff (gain, G) for the monitoring node is the total number of attacks successfully detected known as the 'hit rate' and the total number of falsely classified attacks 'miss rate'. While the payoff for the jammer node is to successfully launch denial of service attack thereby reducing the channel's throughput. This utility function is denoted by {U} = {U1, U2} where U1 = detection rate and U2 = attack gain. Also, U1 = G for the honest node and U2 = 1 – G for the jammer node. This implies that the more detection made, the higher the gain for the honest node and the lower the gain for the jamming node. On the other hand, the more successful attack launched, the higher the gain for the jammer node and the lesser the gain for the honest node. The developed game model is used to establish a compromise between these two known as the Nash equilibrium. Parameters to note includes:

G = Gain for detecting attack
1 – G = Gain for launching an attack (Maximum G = 1)
λ = Attack Gain = 1 – G (Maximum G = 1)
t_c = Time for constant monitoring
t_s = Idle time for monitoring node
$t_p = t_c - t_s$ = Time for periodic monitoring
C_p and C_c = Cost for attack detection during periodic and constant monitoring respectively
C_{cj}, C_{dj}, C_{rj}, C_{rej} = Cost for successfully launching an attack for Constant jamming, Detective jamming, Random Jamming, and Reactive jamming respectively.
T_i = Total jamming time
δT_i= Interval for generating jamming packets
For the reactive jammer once it is activated, it constantly emits jamming signal without intervals thereby acting as a constant jammer. In this case, $C_{rej} = C_{cj.}$

1. For constant jamming, during the continuous monitoring mode we have;

$$t_c\delta T_i[(1 – G) - C_{cj}], t_c(G - C_c) \quad (1)$$

t_c here is the total time the node was on for the access duration.

From the above expression, the first instance implies that the node is on and the attack was successful hence; $t_c\delta T_i$ $[(1 – G) - C_{cj}]$, Since the constant jammer generates signals at intervals, $\delta T_i$is the period of jamming signal interval which has been expressed as a fraction of T_i. While the term 1 – G is the gain for successful attack.

In the second instance; $t_c(G - C_c)$. This simply means that the honest node was able to avert the attack during time $t_c$with gain G and cost $C_{c.}$

For constant jamming, during the periodic monitoring mode we have;

$$t_p\delta T_i[(1 - G) - C_{cj}], \delta T_i[(1 – G) - C_{cj}], t_p(G - C_p) \quad (2)$$

The first term above => $t_p\delta T_i[(1 - G) - C_{cj}]$, shows that the attack was successful even when the monitoring node is on and monitoring.

The second term => $\delta T_i[(1 – G) - C_{cj}]$, shows that the monitoring node is off at this point hence the attack is launched successfully the cost for successful attack and gain is given by (1 – G) and C_{cj} respectively. The t_p term here is null since the monitoring node is not on at this point.

For the third term => t_p (G - C_p) the monitoring node is on and monitoring and the attack was successfully detected. Here, T_i is null since the attack was not successful. The cost for detecting the attack here for the monitoring node is C_p.

2. For deceptive jamming, during the continuous monitoring mode we have;

$$t_c T_i[(1 – G) - C_{dj}], t_c(G - C_c) \quad (3)$$

The first term in $t_c T_i[(1 – G) - C_{dj}]$, implies that the monitoring node is on and the attack was successfully launched. It should be noted that deceptive jammer as stated earlier generates random jamming signal without interval (hence the unavailability of the δT_i term in eqn 3. The cost for successfully launching the attack is given by C_{dj}.

For the second term =>t_c(G - C_c), this simply means that the attack was successfully detected by the monitoring node hence, T_i is null. The cost for successfully detecting the attack here is C_c.

For deceptive jamming, during the periodic monitoring mode we have;

$$t_p T_i[(1 – G) - C_{dj}], t_p(G- C_p), T_i[(1-G) - C_{dj}] \quad (4)$$

The first term =>$t_p T_i[(1 – G) - C_{dj}]$ implies that the monitoring node is on at this point i.e. t_p and the attack was successfully launched with duration T_i (note the absence of δT_i term).

The second term =>t_p(G- C_p) implies that the monitoring node is on and successfully detected the attack. The cost for detecting the attack here is given by C_p.

The third term => $T_i[(1-G) - C_{dj}]$ implies that the monitoring node is not active at this point hence t_p here is null hence, the attack was launched successfully with associated gains as shown.

3. For random jamming, it is known to take up jamming strategy of either the constant jammer or the deceptive jammer. The expression for the random jammer shows that the first two terms, $t_c\delta T_i[(1 – G) - C_{cj}]$ and t_c(G - C_c) has the jammer acting as a constant jammer hence have the same strategy with constant jammer as described above. While during the last two terms, $t_c T_i[(1 – G) - C_{dj}]$ and t_c(G - C_c) the random jammer's strategy is same as the deceptive jammer.

During periodic monitoring, the same is also applicable the first two terms, $t_p\delta T_i[(1 - G) - C_{cj}]$ and $\delta T_i[(1 – G) - C_{cj)}]$ is the same for the constant jammer while the last three terms, $t_p T_i[(1 – G) - C_{dj}]$, t_p(G- C_p) and T_i $[(1-G) - C_{dj}]$ is the same jamming strategy with the deceptive jammer.

4. For reactive jammer, during the continuous monitoring mode we have;

$$t_c\lambda[(1 – G) - C_{rej}], t_c(G - C_c) \quad (5)$$

The first term implies that the jamming attack was successfully launched with gain C_{rej} even though the monitoring node is active at this point. It should be noted that whenever the reactive jammer senses activity in the channel, it activates itself and constantly sends random jamming signal to the channel hence, C_{rej}= C_{cj}.

In the second instance, the monitoring node is active and was able to successfully stop the attack from happening ie. t_c(G - C_c) with cost C_c.

During periodic monitoring we have;

$$\lambda t_p[(1 – G) - C_{rej}], t_p(G-C_p), \lambda[(1 – G) - C_{rej}] \quad (6)$$

The first terms in (6) implies that the monitoring node is active but the attack was successfully launched with cost of C_{rej}.. While the second term =>t_p(G - C_p) implies that the monitoring node was able to detect the jamming attack with cost of C_p.

During the third terms =>$\lambda[(1 – G) - C_{rej}]$, the monitoring node it not active at this point and the jamming attack was successfully launched.

Table 1 Strategy table for the jamming node and (monitoring node) honest nodes.

	M_c	M_p
Con_j	$t_c\delta T_i[(1-G) - C_{cj}]$, $t_c(G - C_c)$	$t_p\delta T_i[(1 - G) - C_{cj}]$, $\delta T_i[(1-G) - C_{cj}]$, $t_p(G - C_p)$
Dec_i	$t_c T_i[(1-G) - C_{dj}]$, $t_c(G - C_c)$	$t_p T_i[(1-G) - C_{dj}]$, $t_p(G- C_p)$, $T_i[(1-G) - C_{dj}]$
Ran_j	$t_c\delta T_i[(1-G) - C_{cj}]$, $t_c(G - C_c)$, $t_c T_i[(1-G) - C_{dj}]$, $t_c(G - C_c)$	$t_p\delta T_i[(1 - G) - C_{cj}]$, $\delta T_i[(1-G) - C_{cj)}]$, $t_p T_i[(1-G) - C_{dj}]$, $t_p(G- C_p)$, T_i $[(1-G) - C_{dj}]$
Rec_j	$t_c\lambda[(1-G) - C_{rej}]$, $t_c(G - C_c)$	$\lambda t_p[(1-G) - C_{rej}]$, $t_p(G-C_p)$, $\lambda[(1-G) - C_{rej}]$

Table 1 shows the strategy table for the two-player non-cooperative mixed strategy game which can be used to form the game theory mitigation framework viz-a-viz the nash equilibrium which is the solution to this research.

3.1 Jamming Game Formulation

As stated, the monitoring node is denoted by A and the jammer node is denoted by B.

The set of strategies available to A = X while that available to B = Y

From Table 2, the strategy matrix can be obtained thus;

Table 2 Mixed strategies

	M_c	M_p
Con_j	a_1 a_2	b_1 b_2
Dec_j	c_1 c_2	d_1 d_2
Ran_j	e_1, e_2	f_1 f_2
Rec_j	g_1 g_2	h_1 h_2

From table 2 we have;

$$X = \begin{bmatrix} a2 & b2 \\ c2 & d2 \\ e2 & f2 \\ g2 & h2 \end{bmatrix} \quad \text{and } Y = \begin{bmatrix} a1 & c1 & e1 & g1 \\ b1 & d1 & f1 & h1 \end{bmatrix}$$

Given the finite set of X above, the probability distribution p assigns a real number p_i called the probability to each outcome i ϵ X such that;

a. $0 \leq p_i \leq 1$ where i = {a2, b2, c2, d2, e2, f2, g2, h2} (7)

and

$$\sum_{i \epsilon X} Pi = 1$$

Also, given a finite set Y above the probability distribution q assigns a real number q_j called the probability to each outcome j ϵ Y such that;

b. $0 \leq qj \leq 1$ where j = {a1, b1, c1, d1, e1, f1, g1, h1} (8)

And

$$\sum_{j \epsilon y} qj = 1$$

From expression 7 and 8, if player A chooses ith strategy from its mixed strategy X and B chooses jth strategy from its mixed strategy Y, the cost for this strategy for A = A_{ij} and the cost for B = $B_{ij.}$

Player A's choices are then given by;

X = {1, …,m} = {a2…h2}

And B's choices are;

Y = {1, …, n} = {a1,…,h1}

A mixed strategy for A is a probability distribution p on the Set of their choices X such that;

$$p.Aq = \sum_{i=1}^{m} p_i (Aq)_i = \sum_{i=1}^{m} \sum_{j=1}^{n} p_i A_{ij} q_j = \sum_{i \in Xj \in Y} A_{ij} p_i q_j \quad (9)$$

While a mixed strategy for player B is a probability distribution q on the set of their choices Y.

To find the expected cost, it is assumed that;

I. Player A uses mixed strategy p
II. Player B uses mixed strategy q
III. Player A and Player B's choices are independent i.e. A's choice does not affect B's choice and vice-versa.

Since the choices are independent, the probability of player A making choice i and player B making choice j is $p_i q_{j.}$

The expected cost to A then becomes;

$$\sum_{i \in Xj \in Y} A_{ij} p_i q_j \quad (10)$$

The expression above means that the probability that player A makes choice i and B makes choice j is $p_i q_{j.}$ The cost to A when this happens is $A_{ij.}$ This value is then summed and multiplied over all the possible choices for both players.

The same holds for player B;

$$\sum_{i \in Xj \in Y} B_{ij} p_i q_j \quad (11)$$

Further details;

Condition 1, if A has a mixed strategy p and B has a mixed strategy q the expected value of A's cost is; p.Aq and for B is p.Bq where A and B represents the strategies.

$$p.Aq = \sum_{i \in Xj \in Y} A_{ij} p_i q_j \quad (12)$$

Also,

$$p.Bq = \sum_{i \in Xj \in Y} B_{ij} p_i q_j \quad (13)$$

Equations 12 can be proven for A by defining Aq as a vector in R^m with components;

$$p.Bq = \sum_{j=1}^{n} A_{ij} q_i \quad (14)$$

Also by definition the dot product of p with Aq is given in equation 14a;

$$p.Aq = \sum_{i=1}^{m} p_i (Aq)_i = \sum_{i=1}^{m} \sum_{j=1}^{n} p_i A_{ij} q_j = \sum_{i \in Xj \in Y} A_{ij} p_i q_j \quad (14a)$$

3.2 Establishing Nash Equilibrium

For this two player game with mixed strategies (pq) one for Player A (honest or monitoring node) and the other for Player B (jammer node). The pair pq is the nash equilibrium if;

1. For all mixed strategy p^1 for player A, $p^1.Aq \leq p.Aq$
2. For all mixed strategy q^1 for player B, $p.Bq^1 \leq p.Bq$

The above conditions imply that player A can't improve its cost by changing its mixed strategy from p to any other mixed strategy p^1. Same is applicable to player B.

Given A's strategy set as {X} and B's strategy set as {Y}, the Nash equilibrium for the jamming game where each player is trying to minimize its cost using mixed strategy is defined below. Here p is defined as the probability of continuous monitoring of the channel and (1-p) is the probability of using periodic monitoring. Also for the jamming node, since in most cases the interval between generated data in constant jamming is almost the same as deceptive jamming, the probability of jamming using either constant, random and deceptive jammer = q while that for reactive jammer = 1 – q the Nash equilibrium is them evaluated as;

$$\alpha = \frac{[tp(1-G)]-Crej}{(1-G)(1-Tc)} \quad (15)$$

$$\beta = \frac{\lambda G - Cc}{G(1-\lambda)} \quad (16)$$

Here α and β are proportional to the attack cost and detection cost respectively. It is also good to note that the attack and detection gains are related by 1-G and G respectively. This means that the higher the detection gain, the lower the attack gains.

4.0 Results

NS-3 network simulator was employed in the implementation of the detection and mitigation framework designed in this work. The different wireless sensor nodes were designed by altering the characteristic of the wireless jamming module of the NS-3 simulator example folder. The transmitting power, idle power, receiving power was designed to comply with the IEEE 802.15.4 radio model (which defines the operation of low-rate wireless personal area networks LR-WPANs). A node was made to act like a jammer node by disabling the associated MAC rules. The different jamming strategies were achieved by varying the jamming intervals respectively. Attack conditions were varied by either changing the traffic interval of the network (ranging from 1s to 10s, with 1s implying fast traffic and 10s implying slow traffic) or by increasing the number of malicious node in the network.

4.1 Discussions

The Nash equilibrium condition shows that the probability of attack detection using continuous monitoring is dependent on the frequency of random data generation hence gain for the reactive jammer. If the channel is continuously sensed busy by the monitoring node, it is likely that the reactive jammer is acting more like a deceptive

jammer (at this point, C_{rej}= C_{dj} for the cost) the honest node's best strategy at this point is to employ continuous monitoring with cost of C_c.

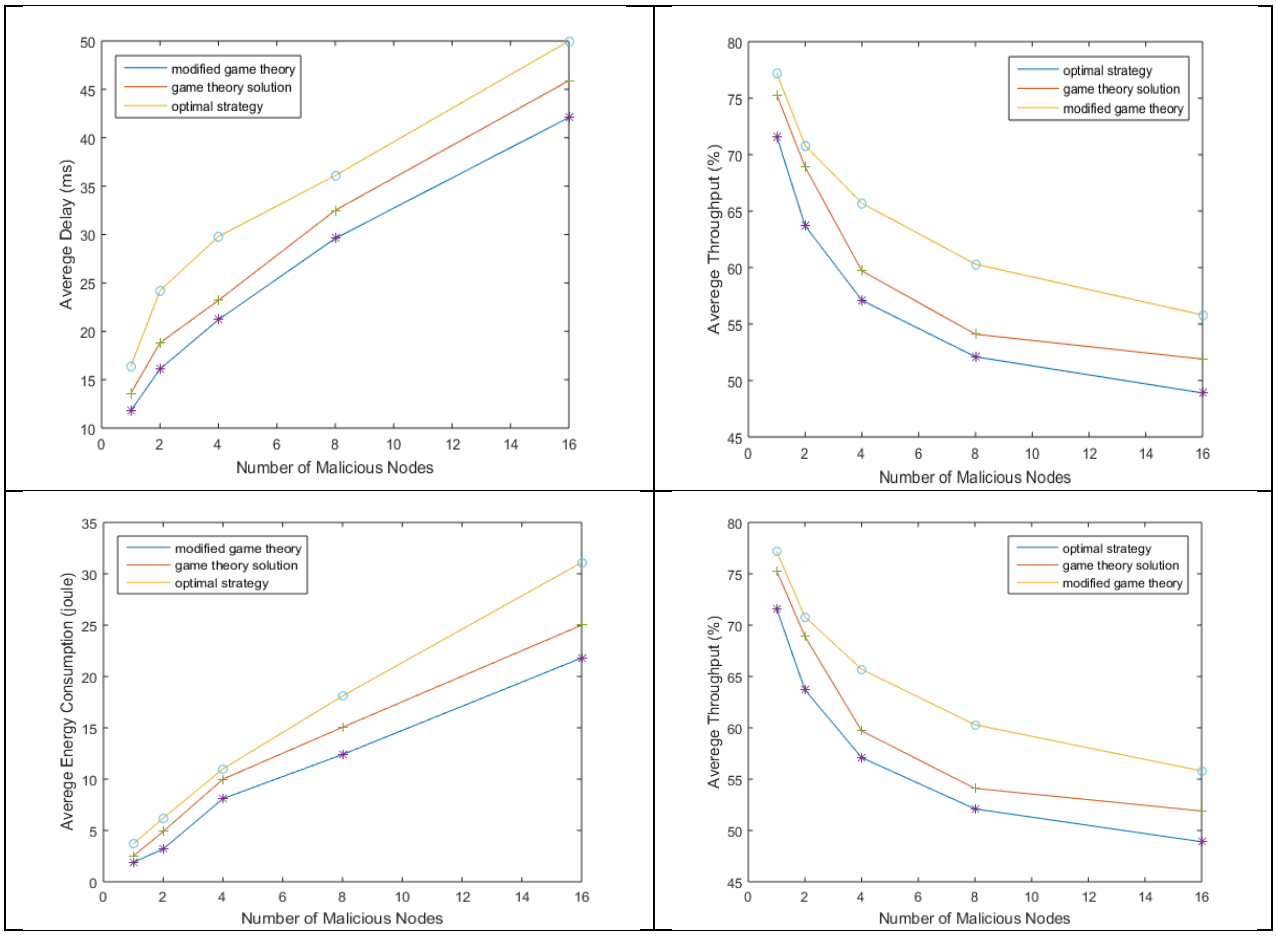


Figure 4.1 Results – varied traffic interval and number of malicious nodes

On the other hand, if the monitoring node constantly employs continuous monitoring, the probability of the jammer using constant jamming or deceptive jamming strategy reduces. The best practice is to employ reactive jamming with gain λ. The associated cost to the monitoring node for detecting the attack here would be C_c which is dependent on λ (being gain for reactive jamming attack). Also when the strategy employed by the monitoring node is periodic monitoring, the best strategy for the jamming node is to use deceptive jamming with hope that it would be sustained (obviously without battery exhaustion) until the monitoring node goes to sleep at this point the attack is successful.

The model has shown a remarkable improvement in average energy consumption, delay and throughput when compared with 'Game theoretic modeling of WSN jamming attack and detection mechanism' developed by (Babar, Prasad & Prasad 2013) and 'Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks' by (Li, Koutsopoulos & Poovendran 2010). It is observed that at maximum number of malicious nodes (16), enhanced game theory solution developed in this work shows a reduced average energy consumption of 11.6% and 27.49% when compared with game theory and optimal strategy solution respectively. The same applies to average delay where there is an improvement of 10.6% and 22% respectively while for average throughput, there is a 13.2% and 19.05% improvement.

5.0 Conclusion and Recommendation

Game theory solution has been employed by economist to model social phenomenon. This study has shown that applying this concept as part of a holistic Intrusion Detection System for wireless sensor networks would improve the overall network performance. By performing a comparative analysis with 'Game theoretic modeling of WSN

jamming attack and detection mechanism' developed by (Babar, Prasad & Prasad 2013) and 'Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks' by (Li, Koutsopoulos & Poovendran 2010) that were reviewed in this work; at maximum number of malicious nodes (16), enhanced game theory solution developed in this work shows a reduced average energy consumption of 11.6% and 27.49% when compared with game theory and optimal strategy solution respectively. The same applies to average delay where there is an improvement of 10.6% and 22% respectively while for average throughput, there is a 13.2% and 19.05% improvement.

It is also recommended that a well designed intrusion detection system should also be associated with this model for optimal performance. The IDS system used for this work was K-Nearest Neighbor which has shown to have a bit noise but the cross-layer features chosen helped for early detection hence timely activation of the mitigation methods discussed in this work. It is recommended for future research to use this mitigation technique alongside a good intrusion detection system. KNN+ or any clustering algorithm that has addressed the inherent problem of K-mean clustering algorithm should be employed.

References

Ajami, S & Teimouri, F 2015, 'Features and application of wearable biosensors in medical care', *Journal of Research in Medical Sciences*, vol 20, no. 2, pp. 1127-1220.

Alotaibi, YK & Federico, F 2017, 'The impact of health information technology on patient safety', *Saudi Medical Journal*, vol 38, no. 12, pp. 1173–1180.

Aswathy, BR, Maneesha, VR, Raghavendra, VK & Hemalatha, T 2012, 'Security Enhancement in Wireless Sensor Networks Using Machine Learning', *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*, IEEE, Liverpool, UK.

Ayaz, M, Ammad-uddin, M, Baig, I & Aggoune, E-HM 2018, 'Wireless Sensor's Civil Applications, Prototypes, and Future Integration Possibilities: A Review', *IEEE Sensors Journal* , vol 18, no. 1, pp. 4 - 30.

Babar, SD, Prasad, NR & Prasad, R 2013, 'Game theoretic modelling of WSN jamming attack and detection mechanism', *International Symposium on Wireless Personal Multimedia Communications, WPMC*, pp. 1-5.

Bhattacharyya, A, Bandyopadhyay, S, Ukil, A, Bose, T & Pal, A 2014, 'Lightweight mutual authentication for CoAP (WIP)', IETF, Kolkata, India.

Danger, J-L, Guilley, S, Hoogvorst, P, Murdica, C & Naccac, D 2013, 'A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards', *Journal of Cryptographic Engineering*, pp. 241-265.

Das, AK 2016, 'A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks', *Peer-to-Peer Networking and Applications*, pp. 234-244.

Dunning, D. (2017, 05 12). What Are the Advantages & Disadvantages of Elliptic Curve Cryptography for Wireless Security? Retrieved 02 23, 2020, from techwalla: https://www.techwalla.com/articles/what-are-the-advantages-disadvantages-of-elliptic-curve-cryptography-for-wireless-security

Duru, C, Aniedu, A, Onyeyili, TI & Alagbu, EEO 2020, 'Modeling of Wireless Sensor Networks Jamming Attack Strategies', *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, vol 67, no. 1, pp. 2313-4410.

Forouzan, BA 2007, *Data Communication and Networking*, McGraw Hill, New York, USA.

He, D, Kumar, N & Chilamkurti, N 2015, 'A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks', *Information Sciences*, pp. 263-277.

Jan, MA, Nanda, P, He, X & Tan, Z 2014, 'A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment', *13th International Conference on Trust, Security and Privacy in Computing and Communications*, IEEE, Beijing, China.

Jiang, Q, Ma, J, Lu, X & Tian, Y 2015, 'An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks', *Peer-to-Peer Networking and Applications*, pp. 1070–1081.

Kalra, S & Sood, SK 2015, 'Secure authentication scheme for IoT and cloud servers', *Elsevier: Pervasive and Mobile*, pp. 210 - 223.

Kumari, S, Li, X, Wu, F, Das, AK, Arshad, H & Khan, MK 2016, 'A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps', *Future Generation Computer Systems*, pp. 56-75.

Li, M, Koutsopoulos, I & Poovendran, R 2010, 'Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks', *TRANSACTIONS ON MOBILE COMPUTING*, IEEE, Barcelona, Spain.

Opeyemi, AO, Attahiru, SA & Gerhard, PH 2018, 'Denial of Service Defence for Resource Availability in Wireless Sensor Networks', *IEEE Access*, vol 6, pp. 6975 - 7004.

Potrino, G, Rango, FD & Faz, P 2019, 'A Distributed Mitigation Strategy against DoS attacks in Edge Computing', *Wireless Telecommunications Symposium (WTS)*, IEEE, New York City, NY, USA.

Riahi, A, Challal, Y, Natalizio, E, Chtourou, Z & Bouabdallah, A 2013, 'A Systemic Approach for IoT Security', *International Conference on Distributed Computing in Sensor Systems, DCOSS 2013*, IEEE, Massachusetts, USA.

Shin, S, Shon, T, Yeh, H & Kim, K 2014, 'An effective authentication mechanism for ubiquitous collaboration in heterogeneous computing environment', *Peer-to-Peer Networking and Applications*, pp. 1-8.

Wang, J, Lin, C-C, Yu, Y-S & Yu, T-C 2015, 'Wireless Sensor-Based Smart-Clothing Platform for ECG Monitoring', *Computational and Mathematical Methods in Medicine*.