Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 20(4): 250-258, Dec. 2022 **Regular paper**

A Cooperative Smart Jamming Attack in Internet of Things Networks

Ashraf Al Sharah[1]*, Hamza Abu Owida[2], Talal A. Edwan[3], and Feras Alnaimat[2]

[1]Department of Electrical Engineering, College of Engineering Technology, Al-Balqa Applied University, Amman 001962, Jordan
[2]Medical Engineering Department, Al-Ahliyya Amman University, Amman 001962, Jordan
[3]Department of Computer Engineering, The University of Jordan, Amman 001962, Jordan

Abstract

The emerging scope of the Internet-of-Things (IoT) has piqued the interest of industry and academia in recent times. Therefore, security becomes the main issue to prevent the possibility of cyberattacks. Jamming attacks are threads that can affect performance and cause significant problems for IoT device. This study explores a smart jamming attack (coalition attack) in which the attackers were previously a part of the legitimate network and are now back to attack it based on the gained knowledge. These attackers regroup into a coalition and begin exchanging information about the legitimate network to launch attacks based on the gained knowledge. Our system enables jammer nodes to select the optimal transmission rates for attacks based on the attack probability table, which contains the most probable link transmission rate between nodes in the legitimate network. The table is updated constantly throughout the life cycle of the coalition. The simulation results show that a coalition of jammers can cause highly successful attacks.

Index Terms: Attacks, Cooperation, Internet of Things, Security

I. INTRODUCTION

By employing Internet of Things (IoT) tools, enterprises may boost their productivity and creativity while also gaining a competitive advantage. IoT devices are used in many applications in different domains, such as smart cities, smart traffic controllers, smart homes, healthcare, and transportation. Many devices with diverse user populations take advantage of these applications. A vast number of IoT devices are interconnected by smart applications, which implies that data interchange and large-scale communication are hampered by the heterogeneous nature of the IoT ecosystem. Consequently, it is an ideal target for a variety of attacks. Because wireless communication is the primary conduit for IoT, practically all wireless communication security issues can spread to IoT networks. Because of the restricted resources and capabilities of nodes in an IoT network, security for such networks is a major concern compared to that for traditional networks. The most common IoT attacks can be classified into the following categories: black hole, wormhole, flooding, sinkhole, Sybil, and jamming. Many types of attacks can affect such networks, which use a wireless medium, making them easier to attack. However, many of these attacks can be easily detected. Jamming attacks are destructive attacks that can interfere with physical transmission and thus the rate at which data is transmitted via wireless communication.

In a black-hole attack, a malicious node advertises to its neighbors that it has the shortest path for the nodes that want to send or forward data; this usually occurs during the routing discovery process.

Received 1 March 2022, **Revised** 11 September 2022, **Accepted** 14 September 2022
***Corresponding Author** Ashraf Al Sharah (E-mail: aalsharah@bau.edu.jo, Tel: +962-797325603)
Department of Electrical Engineering, College of Engineering Technology, Al-Balqa Applied University, Amman 001962, Jordan

Open Access **https://doi.org/10.56977/jicce.2022.20.4.250** print ISSN: 2234-8255 online ISSN: 2234-8883

In a wormhole attack, a malicious node sends the received data to another malicious node via a tunnel, which requires two or more malicious nodes in the same network to collaborate with each other.

In a Sybil attack, malicious nodes generate additional fake nodes with different fake identities; this increases the malicious node's ability to intercept messages routing through the overall network. The malicious node in a sinkhole attack attracts network traffic by advertising to its neighbors that it has the best next hop. Subsequently, this node starts receiving (sinking) all network traffic. Sink nodes do not drop data but monitor all network data; this makes them undetectable to the neighboring nodes. A significant denial of service (DoS) attack known as a jamming attack can disrupt the communication link among a large number of genuine IoT nodes, which affects the performance of the overall network. In general, jamming attacks are among the most harmful attacks that can cripple the communication channels between IoT nodes by presenting counterfeit packets and damaging the communication transmission rates in IoT networks. As a result, this attack poses a significant risk to nodes within IoT networks.

Jamming attacks can be classified into different types: constant, random, deceptive, and reactive jamming attacks. In constant jamming, the jammer continues to produce a high-power signal without following any clear strategy; it simply continues sending a random bit. In random jamming, the jammer switches randomly between sleeping and jamming modes. When this jammer is in sleep mode, it does nothing, and in jamming mode, it acts as a reactive or constant jammer. The jammer in deceptive jamming works almost like a random jammer; the difference between them is that the deceptive jammer sends illegitimate data which appears legitimate to the receiver node to keep the communication channels busy. Reactive jamming can be considered a challenging attack, in which the attacker keeps sensing the channels for available transmissions to activate itself; it remains neutral if the channels remain idle. However, this study does not deal with detection techniques or anti-jamming strategies; rather, it aims to provide researchers interested in jamming attacks with a feasible method of smart jamming for use as a reference. Using a coalition game, we demonstrate a smart jamming attack strategy for IoT networks that may collaborate to assault legal nodes. In this strategy, the attacker node has long been a member of the IoT network. The following are the most significant contributions of this study:

A jamming attack scheme is proposed that relies on a coalition attack for transmission rates observed by the jammers, which is dependent on the attack probability that will come later.

A jamming attack on IoT networks is proposed, which reduces the complexity of individual attacks by offering a lightweight technique. The proposed scheme is a stepwise technique deployed by attackers inside the attacking coalition.

IoT networks can be directly targeted by proposed jamming strategies without any additional users.

The rest of the paper is organized as follows: Section II presents related work, Section III introduces the proposed model and the proposed attacking cases, Section IV discusses the simulation and results, and Section V concludes the study and discusses future work.

II. RELATED WORK

Because we have a limited understanding of how collaborative smart attacks work, there is a shortage of studies in this field that focus on new collaborative smart attacks in the IoT domain. The modeling and analysis of systems under attack has received considerable attention [1-6]. Researchers have illustrated existing attacks and methods to eliminate them. Additionally, work has been done to model threats in the IoT with the aim of studying and analyzing threat capabilities. This has been done by attempting to identify the issue from the perspective of a hypothetical attacker; one common technique is trying to leverage attack trees [7]. Chen [8] described a two-hop system with full-duplex jamming in the presence of a single eavesdropper. According to their findings, full-duplex jamming outperformed a half-duplex system by a wide margin. Chen [9] also discussed the scenario where a base station communicated with a single user in the presence of randomly positioned eavesdroppers. Additional problems for eavesdroppers can be caused by security advancements such as cooperative jamming systems, which broadcast many jamming signals simultaneously.

During a vampire assault, the vampire nodes in the network appear innocent, yet continue to communicate protocol-compliant data to other nodes. Vampire nodes can be observed in two different forms: carrousel and stretch attacks [10]. A situation in which IoT system nodes have varying degrees of relevance was examined by Labib. [11]. The purpose of the jammer is to interfere with an IoT network's performance while remaining undiscovered by limiting the power of its interference according to their own betweenness centrality. One of the most critical attacks on the IoT is a physical attack where the attacker must be close to the network to launch it, whereas a network assault differs significantly in that it does not require the attacker to be close to the network to be launched. A number of physical and network layer attacks have been attempted, such as tampering attack, which involves manipulating the data sent between nodes in an IoT network to manipulate the transferred data between nodes [12].

Table 1. Summary of physical and network attacks with their effects

Layer	Attacks	Description
Network Layer	Sinkhole Attack. [19]	Creates fake routing information, by declaring a shortest path to destination.
	Denial of Service Attack. [20]	Preventing a legitimate node from access, network or services
	Sybil Attack [21]	Malicious node creates a large number of identities of other
	Blackhole attack [22]	Malicious node receives packets and replies with high sequence rather than discard them
	Grayhole Attack [23]	Malicious node agrees to participate in route formation but later it drops packets based on certain conditions
	Wormhole attack [24]	Two or more malicious nodes forward data to each other via a tunnel
	Rushing attack [25]	Malicious node receives route request packet, and immediately forwards it to its neighbors without processing the packet
	Jellyfish attack [26]	Malicious node increases throughput by using alternative route for data packets
Physical layer	Jamming attack [27]	Malicious nodes transmit a radio signal to block legitimate communication by causing intentional interference in networks.
	Tampering [12]	Malicious nodes modify data transferred between nodes
	Fake Node Injection [15]	Malicious control dataflow between nodes
	Scrambling attack [25]	Malicious nodes injection interference using radio frequency to prevent bandwidth allocations
	Replay attack [17]	Malicious nodes keeps network by resending a signed packets many times
	Eavesdropping[25]	Malicious nodes deletes or modifies transmitted data between nodes

It is possible for a malicious node to insert code into the network, which will force the network to shut down, allowing an attacker to take control of that network; this is called malicious code injection [13].

Fake nodes or man-in-the-middle attacks, in which an attacker inserts a fake node between two real nodes in an IoT network. To manipulate the data flow between the nodes [14], algorithms are developed to analyze network traffic and thereby manage linkages and interactions between nodes in legitimate networks to launch an attack on them using traffic analysis, also known as a traffic analysis attack [15]. Through selective forwarding, a malicious node attempts to ensure that only parts of the message are forwarded to the intended recipient [16]. In a replay attack, a malicious node sends a signed packet to the destination numerous times to keep the network busy [17]. Routing information attacks, in which an attacker creates a route or continues to transmit error messages by altering the routing information [18], Table 1 summarize part of physical and network attacks.

III. SYSTEM MODEL

In the current model, which is shown in Fig. 1, the environment is characterized as a coalition-based recurring game with incomplete knowledge. Consider a wireless IoT system with N legitimate IoT nodes connected to each other using any wireless protocol for data transport and sharing. In an IoT network, Nn denotes the number of legitimate nodes, where Nn=[N1,N2,N3…..Nn]. This legitimate network is the attacking surface that is targeted by the smart jammers' coalition. On the other hand, the attacking coalition consists of C jammer nodes, which were previously a part of the legitimate network, where Cn denotes the number of smart jammers and Cn = [C1,C2,C3….Cn]. Each jammer node has a knowledge table; this table was maintained during its stay on the legitimate network, which is why we name it the jammer knowledge table. The duty of the table is to store the updated values of knowledge gained from the legitimate network.

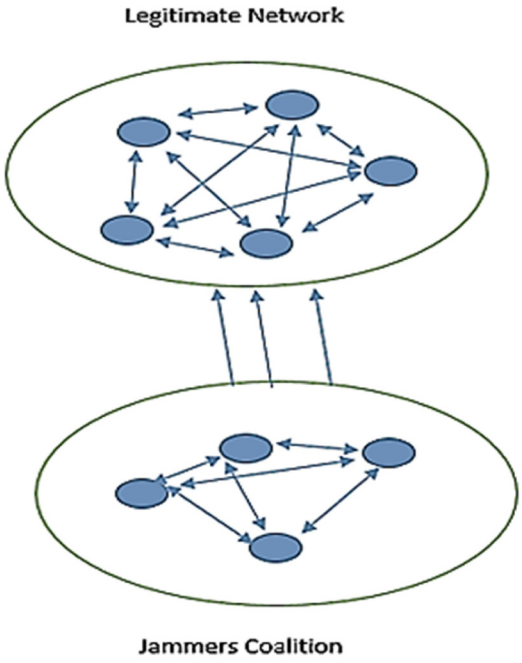


Fig. 1. System model.

After joining the jamming coalition, jammers share the table data with each other. From this data, we use the transmission rates (R) gained by the attacker node during the time. R = [R1,R2,R3,…Rn]. A coalition game is labeled as a pair < C; v >, where C is the set of players in our case set of jammers and v is the characteristic function of any subset S of players where S ⊆ C is called a coalition; C is the grand coalition, which consists of the set of all players. As an example, if we have three players, then there will be eight coalitions (ϕ; (1); (2); (3); (1; 2); (1; 3); (2; 3); C). In general, for C players, the set of coalitions 2C has 2c elements.

A. Coalition Attackers Model

When it comes to network attacks, we assume that there are multiple attackers in the network and that their primary purpose is to disrupt data transmissions between two nodes. As a result, data transmission between nodes is disrupted. At each specified window time (w), the jammers use the jamming attack method based on three separate jamming probabilities, which is described in detail later in section 3, to select a specific channel to attack; this method is then repeated.

B. Attackers Coalition Formation

The attackers' coalition is formed from nodes that have been mitigated from the IoT network to which they previously belonged. When a node joins, it sends or broadcasts a joining signal to other nodes with the same intention, which means that a coalition has already been formed. As of this moment, nodes begin exchanging information with one another in accordance with Algorithm 1. Each time a new member of the coalition joins, the same procedure must be followed (all nodes exchange knowledge regarding the IoT network that was excluded from it). Forming an attackers' coalition has the overall purpose of increasing the effectiveness of the nodes' attacks rather than relying on blind attacks. Consequently, new nodes are needed in the jammers' coalition because old nodes do not know what changes occurred in the IoT network after they left, but this information can be offered by the new nodes, which can then assist the jammers' coalition in estimating the transmission rate hopping procedure after a jammer node leaves.

Fig. 2 shows algorithm 1, which states that the first disjoint attacker node (c1) from the IoT network broadcasts a joining signal for any other disjoint nodes that are interesting in forming an attacking coalition. There should be at least two nodes to testify the coalition formation rules: when two or more attackers exist, they start exchanging the gain information (transmission rates) currently used by the IoT network. This procedure continues throughout the life of the attacker coalition. Let c_n be the number of attackers that join

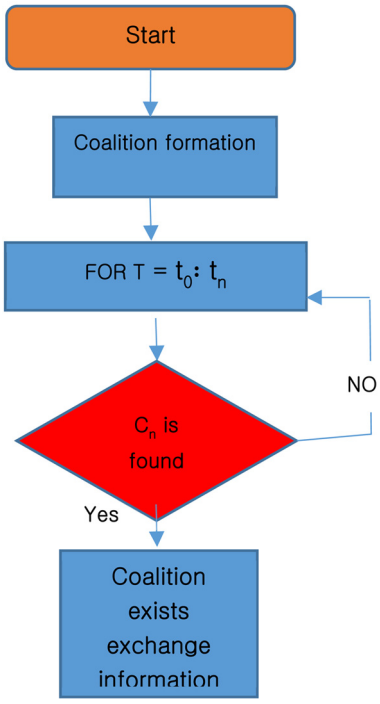


Fig. 2. Algorithm1 for formation of attackers coalition.

the coalition. We can also formulate joining criteria if we are looking for more powerful attacks. Therefore, our criteria is that any node willing to join the attackers' coalition should have knowledge about the transmission rate for at least 15 communication link (NL) between the nodes in the legitimate IoT network; this number can be varied for more flexibility.

$$K_{Cn}(C_{j,i}) = \sum_{i,j \in Nn} O_{ij} \ \ |i,j \geq \mathrm{NL} \tag{1}$$

where $Kcn\ (C_{j,i})$ is the knowledge gained by an attacker node regarding the transmission rate between nodes in a legitimate IoT network, i,j refers to any two connected nodes in the legitimate network, and O_{ij} is the observation by Cn for any two connected nodes in the legitimate network.

C. Surface of Coalition Attack

As previously mentioned, in system mode, the attack surface is a legitimate IoT network, which consists of "N" IoT nodes. These nodes may be legitimate or potential future attackers. The node is a probable future attacker when it leaves the IoT network.

D. Jamming Attack Method

Performing aggressive attacks requires a large amount of

information about the legitimate network transmission rates that have been used for data transmission between nodes, which is achieved by sharing previous knowledge about the legitimate network through the jammers' coalition. This leads to a high potential to damage or corrupt the channels in several time slots. Therefore, this method of attacking urgently is not needed because the attacker nodes are not known for the legitimate network and the jamming probability is high according to their accumulated knowledge. This is the basis of the strength of this method. The attack strategy is computed over a given time window before launching the attack; this window is used to determine if there is any new information from the new joining nodes. Jamming is designed to attack a specific channel between nodes, where O is the number of observed transmission rates performed by the attackers. These observations have been collected over several time windows. These collections is done by using the following equation:

$$O(C), O(C-1), \ldots\ldots\ldots O(C-N+1)$$
$$O(c) = \frac{\sum_{C=O-N+1}^{O}(O(r^2))}{N} \quad (2)$$

where $o(c)$ is the average jammer observation for a given window time, with the number of samples equal to N, denoted as P_o = probability of observations collected by different jammers, and $p_{not\ o}$ = probability of no observations collected by different jammers. We present our method using three different cases to show how we can calculate the attacking probability according to the number of observations gained by the attackers. These probabilities are stored in a table to select the most probable link to the attack. The observation amount can vary according to the time windows. Given that, the transmission rates are captured with probability pr, where

$$\text{pr} = \binom{N}{O(c)} p^{o(c)}(1-\text{p})^{N-o(c)} \quad (3)$$

1) Case 1: For the probability of observations collected by more than 33% and less than 66% of jammers,

In this case, not all jammers have observations for a specific link in the legitimate network; thus, jammers will choose to attack this link with low probability for this window of time according to the attack rate, which is given by

$$W\ (P_{jamming}) = p_o\ ((1 - p_{not\ o}) + p_{not\ o}.\ p_r \quad (4)$$

While not all nodes capture the rate for a specific link, the probability of a successful attack can be utilized by $pr/w(p_o,p_{not\ o})pnoto$. To optimize this problem, the attacking probability is solved by:

$$\max_{p_o\in[0,1]} (p_o, p_{not\ o}) = \frac{pr}{w(p_o, p_{not\ o})} p_o, \quad (5)$$

where

$$w(p_o, p_{not\ o}) \geq NL \quad (6)$$

In addition, because of the lack of information, the jamming probability cannot be further improved subject to the probability of observations. The non-attaching probability is defined as

$$\min_{p_{not\ o}\in[0,1]} (p_o, p_{not\ o}) = \frac{p_r}{w(p_o, p_{not\ o})} p_{not\ o} \quad (7)$$

2) Case 2: For the probability of observations having been collected by more than 66% of jammers but less than 90% of jammers:

In this case, over 66% and less than 90% of jammers have observed a specific link in the legitimate network. Compared to Case 1, jammers will attack this link with a medium probability during the time window. In this case, the probability of a successful attack can be deduced by

$$\frac{p_r}{w(p_o, p_{not\ o})}\ po \quad (8)$$

Referring to the optimum solution of the attacking probability in case 1, we need to characterize the outcome to find the attacking probability $p^*_{o,noto}$ should satisfy that For any strategy p_o,p_{noto}

$$o(c)p^*_{o,}p^*_{noto} \geq o(c)p_o, p^*_{noto} \quad (9)$$

By solving Equation 6, we can obtain the satisfied solutions for the attack as follows:

$$p^*_o = \frac{NL}{1 - p^*_{noto}\ (1 - p_r)} \quad (10)$$

$$p^*_{noto} = \max(p_{noto}) \quad (11)$$

From equations 7 and 10, the observations in case 2 are higher than observations in case 1, which implies that the attack is more efficient in case 2.

3) Case 3: In this case, over 90% of jammers have observations for a specific link in the legitimate network; therefore, jammers will attack this link with a high probability for this window of time.

The probability of success attacks in this case can be calculated by:

$$\frac{p_r}{p_o((w(p_o, p_{not\ o}))}\ p_o \quad (12)$$

In this case, the transmission rate is highly likely to still be in use by the legitimate network, which gives it the highest

possibility to aid in a successful attack; the result for attacking probability can be given by:

$$p_o^* \geq \frac{NL}{1 - p_{not\,o}^* \ (1 - p_r)} \tag{13}$$

$$p_{noto}^* = \min(p_{not\,o}) \tag{14}$$

Note that $p_{not\,o}^*$ in equation 14 is independent of NL and leads to fewer false positives compared to case 2, unless p_{noto}^* both of equations 14 and 11 have the same probability for both cases. It is clear that the observations in Case 3 are the greatest, which implies that the attack in this case is the most efficient.

IV. SIMULATION AND RESULTS

We implemented and proposed an approach using an NS-3 simulator. In the experiments, the attacking surface consists of 150 legitimate nodes, and the simulation consisted of different jammers' coalition sizes (10, 15, 20, and 25) to show that increasing the number of attacker nodes in the attacking coalition leads to improved results. In addition, the impact of jammers was shown as the jammers' coalition increases.

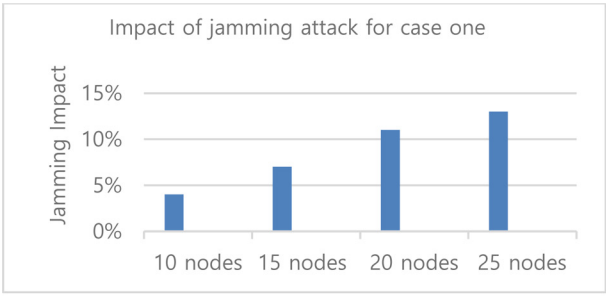
The percentage of successful attacks is shown for each of the three cases, compared with different jammers' coalition sizes. A comparison of the impact factors for the three different cases is shown by comparing each case with different jammers' coalition sizes and comparing the accuracy for the three cases using 25 jammers' collation sizes. Finally, the number of false positives is presented separately for the three different cases with respect to time.

A. Impact of Jamming Attack

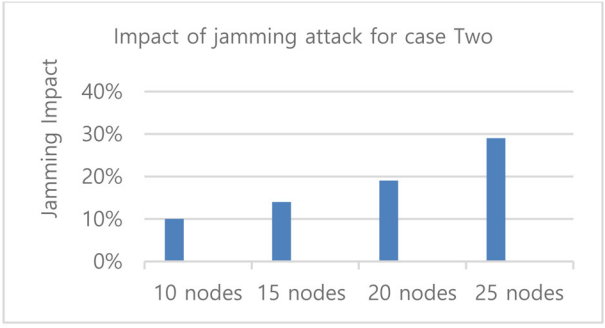
Fig. 3 shows the impact of the jamming attack on the three presented cases with different jamming coalition sizes. It is clearly shown that the impact factor increases as the number of jammers increases in the coalition and the number of observations increases, which thereby increases the attacking probability.

B. Comparison Between Number of Generated Attacks and Number of Success Attacks

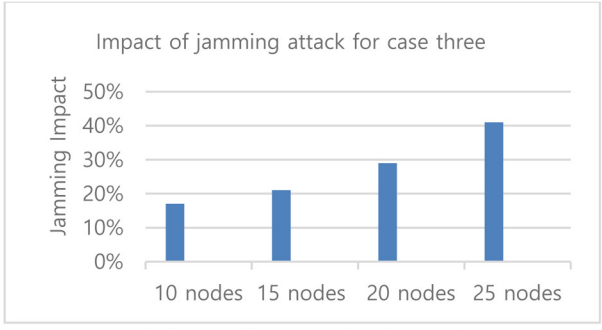
Fig. 4 shows the number of successfully generated attacks according to the total number of generated attacks. It is clear that when there are more nodes in the attackers' coalition, more possible attacks are generated, as shown in the figure. The generated attacks comprise both successful and unsuccessful attacks that have been launched; the figure also shows the differences between the three presented cases with the same simulation time and the same sizes of the jammers' coalition.



(a) Impact of jamming attack for case 1



(b) Impact of jamming attack for case2

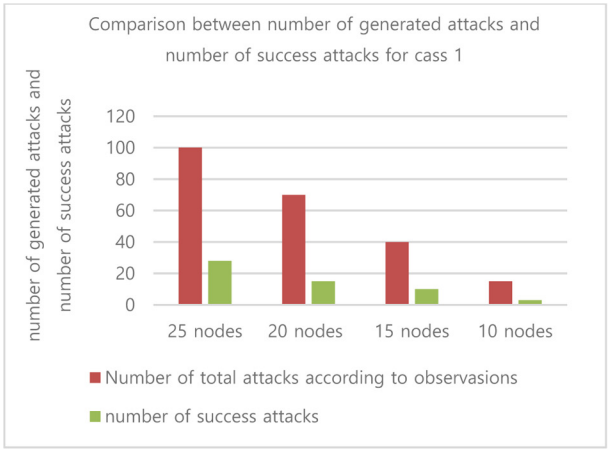


(c) Impact of jamming attack for case 3

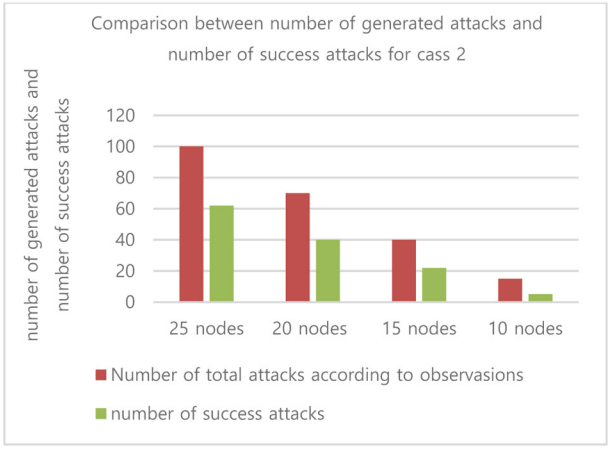
Fig. 3. Impact of jamming attack for three different cases.

C. Transmission Rate Capture Probability VS Number of Observations

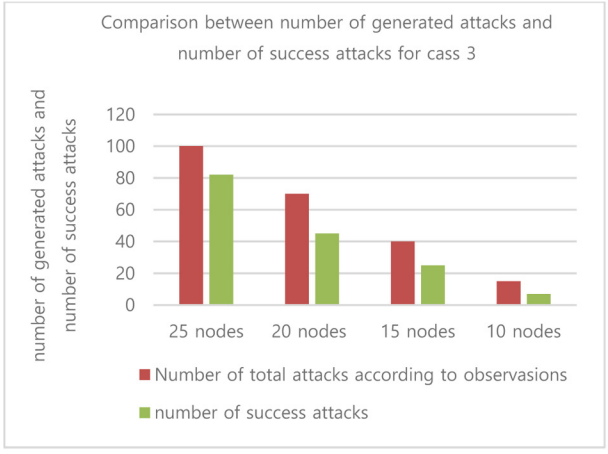
Our findings in Fig. 5 show that the probability of capturing the transmission rate increases when there are more observations in a given window of time; the capturing probability is large when $o(c)$ is greater. Indeed fig. 5 shows $p(r)$ the different $o(c)$. On the other hand, as $p(r)$ increases, the probability of successful attacks increases and the jamming impact is high.



(a) Case 1



(b) Case 2



(c) Case 3

Fig. 4. Comparison between number of generated attacks and number of successful attacks for three cases.

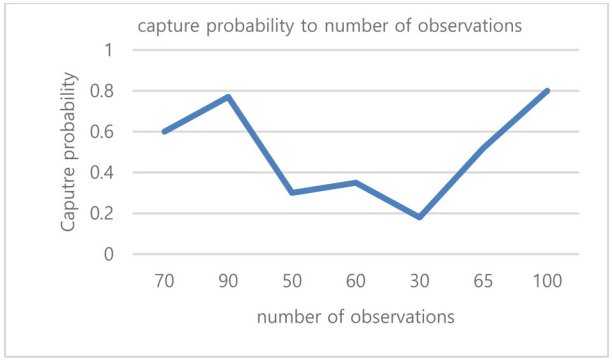


Fig. 5. Transmission rate capture probability as per the number of observations.

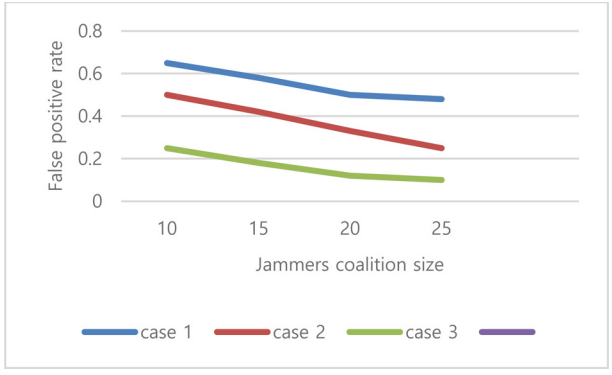


Fig. 6. False positive rate for the three different cases.

D. False Positive Rate

Fig. 6 shows the rate of false positives regarding the cases observed, and it is clearly shown that the rate of false positives increases when the number of jammers decreases. On the other hand, the rate of false positives decreases when the number of jammers increases.

V. CONCLUSION

This study demonstrates that if jammers are mitigated from a legitimate network, they are still able to form a coalition and launch attacks independently. Based on the network's attacking possibility, these nodes have the potential to launch an attack on the legitimate network. Regarding the probability of an attack, three different scenarios were developed, and we were able to demonstrate the effects of the jamming attack carried out by the attacking coalition for each of these three scenarios. In addition, a comparison

between the number of generated attacks and the number of successful attacks was demonstrated. According to our findings, the number of successful attacks was higher than that of isolated attacks, and the false positive rate decreased as the number of attackers increased. Both findings are based on comparisons with solitary attacks. In the future, we intend to analyze the model by expanding it to hundreds of nodes to investigate the proposed strategy in the context of a larger coalition.

ACKNOWLEDGMENTS

This work is supported and sponsored by Al-Balqa Applied University and Al-Ahliyya Amman University.

Persons or institutes who contributed to the papers but not enough to be coauthors may be introduced. Financial support, including foundations, institutions, pharmaceutical and device manufacturers, private companies, intramural departmental sources, or any other support should be described.

REFERENCES

[1] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L. F. Capretz, and S. J. Abdulkadir, "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review," *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022, DOI: 10.3390/electronics11020198.

[2] P. Chen, D. Zhang, L. Yu, and H. Yan, "Dynamic event-triggered output feedback control for load frequency control in power systems with multiple cyber attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 10, pp. 1-13, Oct. 2022. DOI: 10.1109/TSMC.2022.3143903.

[3] X. Jin, S. Lü, C. Deng, and M. Chadli, "Distributed adaptive security consensus control for a class of multi-agent systems under network decay and intermittent attacks," *Information Sciences*, vol. 547, pp. 88-102, Feb. 2021. DOI: 10.1016/j.ins.2020.08.013.

[4] R. Ma, P. Shi, and L. Wu, "Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 5, pp. 2306-2318, Mar. 2020. DOI: 10.1109/TCYB.2020.2975089.

[5] Y. Tian, X. Li, B. Dong, Y. Gao, and L. Wu, "Event-based sliding mode control under denial-of-service attacks," *Science China Information Sciences*, vol. 65, no. 6, Apr. 2022. DOI: 10.1007/s11432-021-3375-5.

[6] X. Huang and X. Wang, "Detection and isolation of false data injection attack in intelligent transportation system via robust state observer," *Processes*, vol. 10, no. 7, p. 1299, Jun. 2022. DOI: 10.3390/pr10071299.

[7] P. Koloveas, T. Chantzios, S. Alevizopoulou, S. Skiadopoulos, and C. Tryfonopoulos, "inTIME: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence," *Electronics*, vol. 10, no. 7, p. 818, Mar. 2021. DOI: 10.3390/electronics10070818.

[8] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574-583, Mar. 2015. DOI: 10.1109/TIFS.2015.2390136

[9] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195-1206, May 2017. DOI: 10.1109/TIFS.2017.2656462.

[10] N. Geethanjali and E. Gayathri, "A survey on energy depletion attacks in wireless sensor networks," *International Journal of Science and Research*, vol. 3, no. 9, pp. 2070-2074, Sep. 2014.

[11] M. Labib, S. Ha, W. Saad, and J. H. Reed, "A colonel blotto game for anti-jamming in the internet of things," in *2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego: CA, USA, pp. 1-6, 2015. DOI: 10.1109/GLOCOM.2015.7417437.

[12] M. N. Aman, M. H. Basheer, S. Dash, J. W. Wong, J. Xu, H.W. Lim, and B. Sikdar, "HAtt: Hybrid remote attestation for the internet of things with high availability," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7220-7233, Aug. 2020. DOI: 10.1109/JIOT.2020.2983655.

[13] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A review on internet of things (IoT)," *International Journal of Computer Applications*, vol. 113, no. 1, pp. 1-7, Mar. 2015. DOI: 10.5120/19787-1571.

[14] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings of 2013 Ninth International Conference on Computational Intelligence and Security*, Emeishan, China, pp. 663-667, 2013. DOI: 10.1109/CIS.2013.145.

[15] L. Basyoni, N. Fetais, A. Erbad, A. Mohamed, and M. Guizani, "Traffic analysis attacks on Tor: A survey," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, Doha, Qatar, pp. 183-188, 2020. DOI: 10.1109/ICIoT48696.2020.9089497.

[16] H. Fu, Y. Liu, Z. Dong, and Y. Wu, "A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks," *Sensors*, vol. 20, no. 1, p. 23, 2020. DOI: 10.3390/s20010023.

[17] G. Rajendran, R. R. Nivash, P. P. Parthy, and S. Balamurugan, "Modern security threats in the Internet of Things (IoT): Attacks and countermeasures," in *2019 International Carnahan Conference on Security Technology (ICCST)*, Chennai, India, pp. 1-6, 2019. DOI: 10.1109/CCST.2019.8888399.

[18] S. Choudhary and N. Kesswani, "Detection and prevention of routing attacks in internet of things," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, New York: NY, USA, pp. 1537-1540. DOI: 10.1109/TrustCom/BigDataSE.2018.00219.

[19] R. Baskar, P. C. K. Raja, C. Joseph, and M. Reji, "Sinkhole attack in wireless sensor networksperformance analysis and detection methods," *Indian Journal of Science and Technology*, vol. 10, no. 12, pp. 1-8, May 2017. DOI: 10.17485/ijst/2017/v10i12/90904.

[20] T. Jamal, Z. Haider, S. A. Butt, and A. Chohan, Denial of service attack in cooperative networks, 2018, [Online] Available: arXiv:1810.11070, 2018.

[21] A. Rajan, J. Jithish, and S. Sankaran, "Sybil attack in IOT: Modelling and defenses," in *Proceedings of 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 2323-2327, Udupi, India, 2017. DOI: 10.1109/ICACCI.2017.8126193.

[22] N. Panda and B. K. Pattanayak, "Analysis of blackhole attack in AODV and DSR," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 5, pp. 3092-3102, Oct. 2018. DOI: 10.11591/ijece.v8i5.pp3092-3102.

[23] M. Jeevamaheswari, R. A. Jothi, and V. Palanisamy, "AODV routing protocol to defence against packet dropping gray hole attack In MANET," *International Journal of Scientific Research in Science and Technology*, Jun. 2018.
[24] S. Deshmukh-Bhosale and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based internet of things," *Procedia Manufacturing*, vol. 32, pp. 840-847, 2019. DOI: 10.1016/j.promfg.2019.02.292.
[25] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616-644, Nov. 2019. DOI: 10.1109/COMST.2019.2953364.
[26] A. Malik, S. Gautam, S. Abidin, and B. Bhushan, "Blockchain technology-future of IoT: Including Structure, limitations and various possible attacks," in *Proceedings of 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, India, pp. 1100-1104, 2019. DOI: 10.1109/ICICICT46008.2019.8993144.
[27] N. Namvar, W. Saad, N. Bahadori, and B. Kelley, "Jamming in the internet of things: A game-theoretic perspective," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington: DC, USA, pp. 1-6. DOI: 10.1109/GLOCOM.2016.7841922.

Ashraf Al Sharah
Ashraf Al Sharah has completed his PhD from Tennessee State University. USA. He was a research associate at cyber vis research lab. And served as an Assistant Professor in the Department of Computer Engineering at Al-Ahliyya Amman University. He is serving now as an assistant professor in electrical engineering department in Al-Balqa Applied University. His research interest include wireless security, IoT, smart attack and game theory.

Hamza Abu Owida
Hamza Abu Owida has completed his PhD from Keele university , UK. He was a postdoctoral Research Associate: Developing xeno-free nanofibrous scaffold methodology for human pluripotent stem cell expansion, differentiation and implantation towards a therapeutic product, Keele University, Institute for Science and Technology in Medicine (ISTM), Staffordshire /UK. He is assiosiate professor in medical engineering department in Al-Ahliyya Amman University . He has published more than 30 papers in reputed journals.

Talal A. Edwan
Talal A. Edwan has completed his PhD from Loughborough University UK. He served as an Assistant Professor in the Department of Computer Engineering at PSUT 2014-2019., and as an Assistant Professor in the Department of Computer Engineering at Al-Ahliyya Amman University (AAU) 2020-2022. He is now an Assistant Professor in the Department of Computer Engineering at the University of Jordan. His research interests are: Computer Networks, Network Congestion Control, Performance Evaluation/Engineering of Computer Systems/Networks and Queueing Theory.

Feras Alnaimat
Feras Alnaimat has completed his PhD from University of Birmingham, Birmingham, UK. In 2018, he joined the department of Medical Engineering, Al-Ahliyya Amman University, as an assistant professor. His current research interests include design of artificial disc implant, artificial joints and bio fluid mechanics. He is one of the steering committee of the Innovation and New Trends in Engineering, Science and Technology Education Conference.