Volume 1 (2026), Issue 2
pp. 69–85

TSARKA SCIENCE

eISSN: 3134-6057
pISSN: 3134-6049

DOI: 10.66571/tsarka-3134-6057-08

USING GAME THEORY IN WIRELESS NETWORKS FOR NETWORK SECURITY

A. Shahidani[1*], A. Shaikhanova[1], G. Bekeshova[1], L. N. Abdullah[2]

[1]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

[2]Universiti Putra Malaysia; Serdang, Selangor, Malaysia

*Corresponding author: aigul.shaikhanova@gmail.com.

Abstract

Wireless sensor networks (WSNs) are widely applied in environmental monitoring, health care, smart cities, industrial control, and many other domains due to their flexibility and low cost. Typically, WSNs are organized as mesh networks in which each node collects data, transmits it to its nearest neighbors, and simultaneously operates as a relay for other nodes. This cooperative data transmission is the central mechanism that maintains the stability and functionality of the entire system. Nevertheless, the increasing deployment of WSNs has made them an attractive target for adversaries. Both passive attacks, such as eavesdropping or traffic analysis, and active attacks, including denial of service, spoofing, or selective forwarding, pose serious threats to secure and efficient communication. These attacks not only affect data confidentiality and integrity but can also disrupt network availability, causing failures in critical services. Therefore, ensuring strong security mechanisms has become a fundamental requirement for WSNs. One of the most promising approaches to address these challenges is the development of intrusion detection systems (IDS). An effective IDS must be designed with consideration of the specific communication patterns, resource limitations of sensor nodes, and the wide range of potential attack scenarios. Such adaptive solutions can provide timely detection, responsive countermeasures, and significantly improve the resilience of wireless sensor networks.

Keywords: *wireless sensor networks, mesh networks, cooperative communication, network security, passive attacks, active attacks, intrusion detection systems.*

1. Introduction

A wireless sensor network is a type of network that consists of energy-efficient and multifunctional sensor devices equipped with wireless communication with a small range of radio waves, which are used to monitor the physical world [1]. In some cases, a wireless sensor network can be formulated from a single cluster. In a more

TSARKA SCIENCE
Volume 1 (2026), Issue 2
pp. 69–85
eISSN: 3134-6057
pISSN: 3134-6049

demanding environment, a wireless sensor network is divided into multiple clusters for simplified management of multiple nodes and high-quality network traffic. Each cluster consists of multiple sensor nodes and one master node, which sends all data collected from the sensor nodes to the base station. The base station is the central control system of the wireless sensor network. The architecture of the wireless sensor network is illustrated in Figure 1.

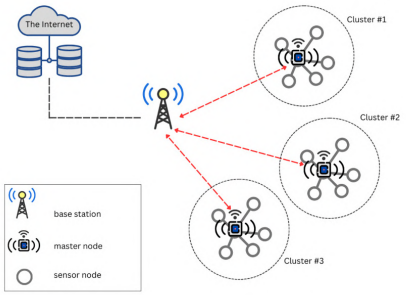

Figure 1. Architecture of simple wireless sensor network

Wireless sensor networks (WSNs) have evolved into a pivotal technology across various sectors, encompassing environmental monitoring, smart homes, and beyond, primarily due to their versatility, scalability, and cost-effectiveness [2,3]. These networks, characterized by the absence of physical connections, facilitate seamless interactions among devices at any place and time, significantly advancing user technology and the Internet of Things (IoT) to simplify daily processes. Despite the widespread adoption of WSNs, they inherently pose significant security risks, attributed to their open communication nature, making them susceptible to diverse cyber-attacks.

The introduction of game theory into the domain of network security offers a sophisticated strategy to preempt and mitigate potential threats effectively. This approach utilizes the predictive capabilities of mathematical models to simulate the strategic interactions between network defenders and potential attackers, thus providing a novel perspective on enhancing the resilience of WSNs against such threats.

Wireless networks, particularly those integrated with IoT devices, face the challenge of ensuring data transmission while contending with inherent functional differences from wired networks [4,5]. These differences include mobility and trivial connection facilitated by the lack of physical cables, broadening their application in communication. However, this convenience comes with a lowered level of security, as devices within a wireless network share a common communication channel, exposing them to potential traffic interception and misuse if data encryption technologies are inadequately applied. Furthermore, suspicious devices within these networks may exploit

Volume 1 (2026), Issue 2
pp. 69–85

TSARKA SCIENCE

eISSN: 3134-6057
pISSN: 3134-6049

the radio spectrum or other system resources to launch denial-of-service (DoS) attacks, exacerbating security concerns.

2. Purpose and objectives of the study

The study focuses on the unique vulnerabilities inherent in IoT devices due to their limited system resources and reliance on low-power network protocols. These constraints make them susceptible to various attacks, notably DoS attacks, which compromise service by flooding the network with unnecessary packets, thus draining resources and increasing power consumption. This research examines the role of game theory in enhancing the security and operational efficiency of wireless networks under such threats. By considering devices as rational agents within a game-theoretical framework, this approach aims to simulate attack scenarios and formulate strategic defenses.

The primary goal is to leverage the principles of game theory to develop a comprehensive understanding of attack dynamics and defense mechanisms within wireless networks. This involves analyzing the behavior of network nodes as players in a game, identifying potential vulnerabilities, and crafting strategies that mitigate the risks posed by security threats. Through game theory analysis of various attack scenarios, the study seeks to pinpoint effective methods for detecting and neutralizing threats, thereby safeguarding network communications against the evolving landscape of network vulnerabilities.

In doing so, the research underscores the potential of strategic decision-making in establishing resilient defense systems against network attacks, emphasizing the critical role of game theory in the realm of wireless network security.

3. Methods and Materials

In wireless networks, devices (i.e., nodes or players) are programmed to follow a protocol and these devices are rarely reprogrammed to change the protocol. Thus, these nodes are rational individuals who make decisions following network protocols. Using game theory, simulation of attack scenarios in wireless networks can demonstrate the rational behaviors of nodes [6]. Depending on the network architecture and the constituent infrastructure parameters, certain types of games are applied to characterize the application of game theory in wireless networks. Classification and comparison of wireless network structures simplify the understanding of simulation and reasoning scenarios. The presented simulations of RPL protocol in two different scenarios reveal the normal functioning of the network and the attack implemented by a suspicious node in the network. The Cooja simulation tool and Contiki OS were used in the simulation process [7]. A generalized security game was simulated to demonstrate the decision-making process between the suspicious node, the local IDS, and the global IDS. This game has been adjusted to account for the effectiveness of the local IDS and global IDS to demonstrate the role of the trust mechanism

TSARKA SCIENCE
Volume 1 (2026), Issue 2
pp. 69–85
eISSN: 3134-6057
pISSN: 3134-6049

between systems in wireless networks.

Primarily, the simulation of an attack in a single wireless sensor network cluster is demonstrated to understand the rational behavior of systems. As an attack implementation experiment, devices transmitting data over the RPL protocol have been added to the simulation tool. RPL (IPv6 Routing Protocol for Low-power and Lossy Networks) is a distance vector protocol designed for IPv6-based devices with limited system resources. RPL protocol operates on the IEEE 802.15.4 standard with support for 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network), which is a component of the adaptation layer of routing before data transmission. The 6LoWPAN adaptation layer provides sensor devices with IP protocol establishment to construct network availability. The adaptation layer plays an important role in implementing routing protocol at the network layer and representing end-to-end communication between devices.

One of the common types of DoS attacks is a flooding attack [8,9]. It is implemented by sending a large number of connection generation requests by an attacker or suspicious node to deplete the resources of legitimate nodes. In this case, the connection request is sent to the transport layer of the protocol to transmit data to neighboring nodes. An intruder or suspicious node in the network repeatedly sends connection requests to neighboring legitimate nodes for a particular period till the full realization of denial of service. As a result of this scenario, legitimate nodes dispose of system resources and become inactive when resources run out. If the intruder is an insider (i.e. one of the legitimate nodes in the network), this node also disposes of all system resources by sending a large number of connection requests and goes into inactive mode after complete resource utilization.

Contiki OS and the network traffic simulation tool Cooja [10] were used to simulate this attack in a single wireless sensor network cluster. To compare the effects of the attack, the simulation was implemented in two phases: the normal operation of RPL protocol traffic and the process of traffic congestion due to forwarding a large number of packets from an insider node. The Cooja simulation tool consists of categorized functionality: a network architecture visualization tab, a window for monitoring network traffic, a control panel for setting the simulation timer, and tabs for writing scripts.

1)Simulation of the normal functioning of the RPL protocol.

In the first scenario, the cluster consists of one main node in the cluster (#1, green node) and ten normal legitimate nodes (#2-11, yellow nodes). When localizing nodes, the range of radio waves that are covered around each node must be taken into account. In the network architecture tab, one cell illustrates one meter of network range. Given the scale of the radio wave coverage capability, all nodes were arranged accordingly. In a cluster, normal nodes connect to forward data to the master node.

Volume 1 (2026), Issue 2
pp. 69–85

TSARKA SCIENCE

eISSN: 3134-6057
pISSN: 3134-6049

Accordingly, the master node sends all collected data to the base station. However, the base station is not considered in the simulation to simplify the process of reasoning interactions between nodes. The timer was set to 100,000 milliseconds in the RPL protocol simulation in standard operation (Figure 2).

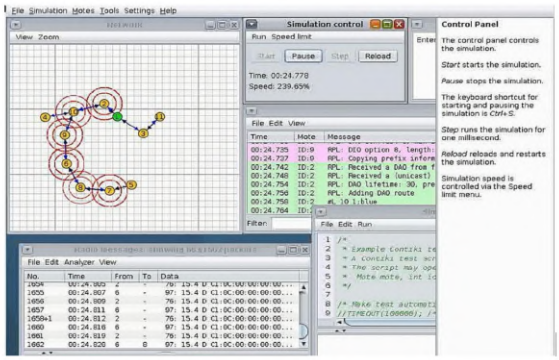

Figure 2. Simulation of a normal functioning of RPL protocol

In the traffic monitoring tab, the process of the RPL protocol and the types of packets transmitted between nodes during normal network operation are displayed. After the timer ends, the traffic result has been saved as a .pcap file for further analysis. Additional packet monitoring and analysis tools can be used to fully analyze and re-examine the traffic. In this simulation, the Wireshark traffic monitoring tool was used. By opening a .pcap file in Wireshark, the packets can be analyzed directly or converted to any other file format. The file was saved in .csv format to make it easier to view packets in linear order. The first column of the .csv file defines the numbering of packages starting from 1 to 5719. As shown in the figure (Figure 3), the total number of packets transmitted over the network comprised 5719 packets. The next columns represent data about the IPv6 format address, the type of message being transmitted (ICMPv6) between nodes, the name of the protocol being executed (the RPL protocol), the ICMPv6 message format (SYN, ACK, SYNACK, etc.) and the DODAG information object packets being transmitted.

Figure 3. Inspection of packets in the first scenario

TSARKA SCIENCE
Volume 1 (2026), Issue 2
pp. 69–85
eISSN: 3134-6057
pISSN: 3134-6049

2) Simulation of the flooding attack.

In the second simulation scenario, nodes exchange data according to the RPL protocol. However, the cluster consists of one master node (#1, green node), regular legitimate nodes (#2-10, yellow nodes), and one suspicious legitimate node (#12, pink node). The red circles around the node indicate high-quality data transmission capability, and the green circles indicate the detection range of neighboring nodes. Blue arrows between nodes illustrate packet transmissions from one node to another. In the simulation, a suspicious node is treated as an insider that has been attacked by an outsider. The outsider tries to implement an attack after gaining access to one legitimate node in the cluster. Spoofed packets are sent to normal legitimate nodes from the suspect node to deplete system resources and overload network traffic. After arranging all nodes to the appropriate scale, the timer was set to 100,000 milliseconds. The simulation process is illustrated in the figure (Figure 4).

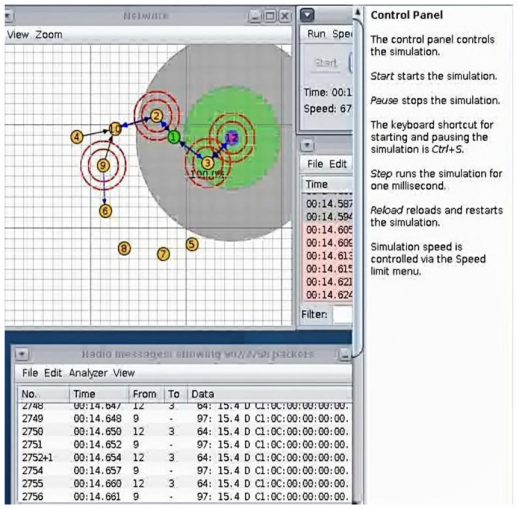

Figure 4. Simulation of Flooding attack in RPL protocol

All traffic was captured in a .pcap file for further analysis. Consequently, this file was converted to a .csv file using the Wireshark tool. The first column of the .csv file shows the sequence of packets numbered from 1 to 51376. As shown in Figure 5, the total number of packets transmitted over the network amounted to 51376 packets. The following columns show the IPv6 address, the type of message (ICMPv6) transmitted between nodes, the name of the protocol to run (RPL protocol), the ICMPv6 message format (SYN, ACK, SYNACK, etc.), and the DODAG information object packets transmitted.

Volume 1 (2026), Issue 2
pp. 69–85

TSARKA SCIENCE

eISSN: 3134-6057
pISSN: 3134-6049

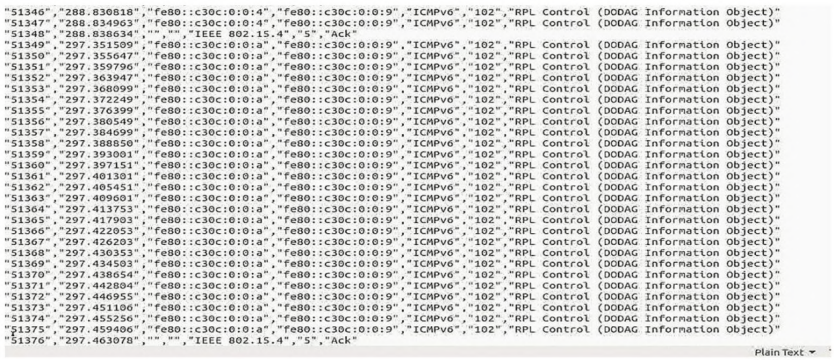

Figure 5. Inspection of packets in the first scenario

Due to congested traffic, the number of packets transmitted reached the maximum level. The number of transmitted packets in the attack scenario was nine times higher than the normal operating network traffic. The suspicious node (#12) sends spoofed packets to the master node (#1) as well as the normal nodes (#2 and #3). Subsequently, these nodes forward the spoofed packets to other neighboring nodes. As a result, the suspicious legitimate node depletes the system resources of the regular legitimate nodes to realize the denial of service of this cluster. Comparing the results of the two simulations based on the number of packets, the nodes utilize nine times more system resources by the impact of the flooding attack. As a result, normal legitimate nodes go into inactive mode after depleting resources. And on the other hand, the suspicious legitimate node also utilizes its own system resources by implementing this attack and forwarding unnecessary packets, and finally, this node also goes into inactive mode after system resources are completely exhausted.

In order to simulate the attack, conceptual schemes of academic work by Alex D'Hondt et.al (2015) [11] were used which consist of designed simulations of three different types of attacks in wireless sensor networks: Flooding attack, Increased version attack, Decreased rank attack. The conceptual schemes of the simulation data directly focus on the interaction of a suspicious legitimate node with regular legitimate nodes in the same cluster. In comparing the two stages of the simulation, it was determined that the mechanisms for detecting and preventing congestion in the network are not present in the RPL routing protocol in wireless networks. Therefore, network congestion detection and prevention mechanisms depend on understanding the concept of interconnected system behaviors (i.e., nodes) in different scenarios. Network congestion detection mechanisms must be included in the local IDS and the global IDS with RPL support given the interaction between present nodes in the same cluster. Interconnected node behaviors can be formed by strategic reasoning using the concept of game theory.

When modeling wireless networks with a priority on security, we need to consider

TSARKA SCIENCE

Volume 1 (2026), Issue 2
pp. 69–85

eISSN: 3134-6057
pISSN: 3134-6049

the rational behaviors of the nodes that operate on the protocol and the complexity of the network technology. According to different network technologies, Chen et al. [12] proposed a systematic concept of game theory in wireless networks which consists of four categories: prevention of DoS or DDoS attacks, intrusion detection, security hardening, and interaction with suspicious or malicious nodes. Given the interaction between nodes in the network, modeling scenarios with the potential presence of an insider among the nodes play a key role to strengthen security technology by strategically reasoning about the operation of systems in the network.

In attack implementation scenarios, the attacker makes the decision first (i.e., to attack or not to attack) and is the dominant player (i.e., the player with the dominant strategy) in security games. In this case, Stackelberg's game concept is suitable for modeling the game with one dominant player. Given this characteristic of the Stackelberg game, the interaction between the three kinds of systems was formed as a game.

The following basic parameters of the game must be defined to form a game:

1)Number of players. There are three players in the game: the attacking node, the local IDS, and the global IDS. This game is based on sensor devices in wireless networks with IDS (Intrusion Detection System) functionality, which utilizes minimal system resources and has a less complex structure compared with the standalone IDS. The local IDS is installed in every node including regular nodes and a master node. Each node with local IDS functionality proposes a suspicion or trust assertion to neighbor nodes in the cluster and sends data with the specific statement to the master node. In turn, the master node of each cluster forwards this data to the base station. Global IDS is installed in the base station, which makes the final decision to exclude a particular node from the network or accept the node into the network. On the other hand, the attacking node is treated as a legitimate node in the network which has been attacked by an outsider, and consequently, the attacker's goal is to implement the attack as an insider.

2)The range of strategies of each player. Each player in the game has two strategies respectively. Strategies of the attacking node: attack realization and normal behavior (i.e., attack and normal). Strategies of the local IDS: suspicion statement and trust statement(i.e., suspicion and trust). Strategies of the global IDS: exclusion of a suspicious node from the network and acceptance of suspicious node behavior (i.e., exclusion and acceptance).

3)Availability of information about potential attacks. At the beginning of the game, players do not have information about the strategies of other players. The suspicious node may have access to information about the defense functionalities of the local IDS and the global IDS. On the other hand, the local IDS and global IDS have no information about the potential attack. However, the local IDS and global IDS will save all

Volume 1 (2026), Issue 2
pp. 69–85

TSARKA SCIENCE

eISSN: 3134-6057
pISSN: 3134-6049

information about the progress of the game and the past actions of the suspicious node to form optimal strategies in the next rounds of the game.

4)Strategy combination outcomes. Since there are three players in the game, and each player has two strategies, therefore, the total number of resulting strategy combinations is 8 (i.e., 2×2×2 = 8).

5)Indicators of a player's benefits in choosing each strategy. Determining the indicators of strategic advantage is a key component for the calculation of Nash Equilibrium. In this game, the player's benefit indicators for each strategy choice range from 0 to 1; 0 denotes a less favorable strategy (i.e., with a minimum win rate), and 1 denotes a more favorable strategy (i.e., with a maximum win rate).

The most common tool for forming a game and calculating the Nash Equilibrium is the Gambit game theory tool [13] developed by the California Institute of Technology. Gambit supports normal and extended-form games with a finite outcome and does not support infinite games. Normal-form games are illustrated in a table, while extended-form games are illustrated in a tree structure. Gambit was used to visualize the constructed game and calculate the Nash Equilibrium.

Extended-form games are used to form games with sequential moves where. the players do not act simultaneously but in turn. Given the number of players in the game, the game diagram has an extended form; players are defined by a circular form, and branches coming out of the circular form illustrate player strategies.

Each player has an information set presented as "player ID: player round ID". Since the attacking node is the dominant player (i.e., starts the game first), in the diagram this player is located at the root of the structure displayed as red. The attacker's information set is displayed as 1:1 (i.e., the first round of the first player's turn). And also, the local IDS is illustrated as blue and has the information set as 2:1 (i.e., the first round of the second player's turn) and 2:2 (i.e., the second round of the second player's turn). The global IDS is displayed in yellow and the information set consists of two parameters: 3:1 and 3:2.

Any IDS technology does not have 100% accuracy in intrusion detection. Because of this fact, the information sets of local IDS and global IDS are connected by a dotted line to visualize the relationship between true and false intrusion probabilities. After forming the game, the payoffs of players for each strategy combination were added in the form of rational numbers. The payoffs are located at the very end of the branches on the right side of the structure, according to each possible combination of strategies. The scheme of the generated game is shown in the figure (Figure 6).

TSARKA SCIENCE
Volume 1 (2026), Issue 2
pp. 69–85
eISSN: 3134-6057
pISSN: 3134-6049

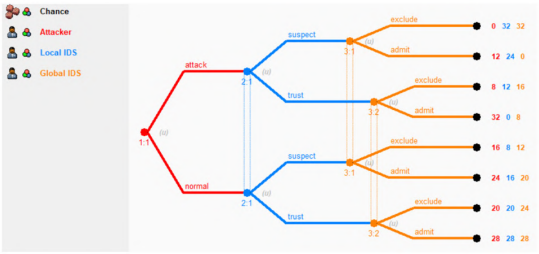

Figure 6. Formulation of the game using Gambit

The attack detection capabilities of both IDS systems were not considered in this game. However, in real infrastructure, attack detection capability metrics are not calculated at 100% and the detection probability of a potential attack varies depending on the detection efficiencies of IDS systems. A low-performing local IDS in resource-limited systems may generate false alerts and overload the main IDS or not detect an attack in the network at all. Given this fact, in the next section, the attack detection efficiencies of both IDS systems are considered to understand the trust mechanism between the local IDS and the global IDS. To strengthen the trust between the systems, the attack detection efficiencies of both IDS systems should have a high detection probability to distinguish the attack scenario from the normal behavior of the systems.

According to the results of the game, the presented reasoning about the interconnected strategies of the players is correct. The development of the players' course of action is marked in black at the branch level illustrating the strategies of the players. Also, the probabilities of accepting certain strategies are shown in the range from 0 to 1 for each player. As a result, using the technique of determining dominant strategies, two Nash Equilibria were obtained: attack, suspicion, exclusion = (0, 32, 32) and norm, trust, acceptance = (28, 28, 28). The resulting game results are shown in the following figure (Figure 7).

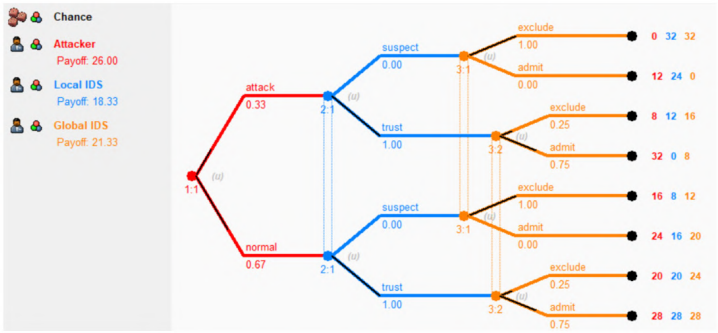

Figure 7. Solution of the game

Volume 1 (2026), Issue 2
pp. 69–85

TSARKA SCIENCE

eISSN: 3134-6057
pISSN: 3134-6049

The previous security game between the attacker node, local IDS, and global IDS is presented considering the probability of attack detection. The BoT-IoT dataset created in the Cyber Range Lab of UNSW Canberra [14] was used to refine the probability of attack detection. In this dataset, the network environment of Internet of Things devices consists of a combination of data obtained from the network traffic during normal network operation and an attack scenario. The attack detection efficiencies of the two system IDS algorithms were evaluated using this dataset. Naive Bayes algorithm was used for the local IDS and Random Forest algorithm was used for the global IDS. Alert metrics in IDS systems are determined based on the reality and falsity of the attack for different scenarios. A matrix of alert types was allocated to eight combinations of metrics when evaluating the performance of the two IDS systems. The matrix consisting of alert metrics is presented in the following table (Table 1).

Table 1. Matrix of detection metrics

Positive	Negative class
True-positive (TP)	True-negative(TN)
False-positive (FP)	False-negative (FN)

Detailed description of the types of detection metrics:

1) True-positive (TP): detection of an attack;

2) True-negative(TN): detection of the absense of an attack;

3) False-positive (FP): sending false warning about an attack;

4) False-negative (FN): undetection of a real attack.

Using the BoT-IoT dataset, the Naive Bayes and Random Forest algorithms in IDS systems were evaluated to generate a combination of alerting metrics. Payoffs of the local IDS and the global IDS were adjusted by considering the detection probabilities in the two algorithms. The detection probabilities were considered as the performance of these systems.

Adjusting the payoffs of both IDS systems to account for the detection efficiency of a real attack from the normal functioning of the systems and network can demonstrate the close relationship between local IDS and global IDS and the importance of the detection efficiency of both systems. The adjusted payoffs of IDS systems considering attack detection efficiency for each combination of alerting metrics are presented in the following table (Table 2).

TSARKA SCIENCE
Volume 1 (2026), Issue 2
pp. 69–85
eISSN: 3134-6057
pISSN: 3134-6049

Table 2. Comparison of payoff in two scenarios

	Efficiency rates of IDS		Payoffs of local IDS and global IDS without efficiency rates of intrusion detection		Payoffs of local IDS and global IDS considering efficiency rates of intrusion detection	
	Local IDS	Global IDS	Local IDS	Global IDS	Local IDS	Global IDS
TP-TP	0.95	0.99	32	32	30.4	31.68
TP-FN	0.95	0.01	24	0	22.8	0
FN-TP	0.05	0.99	12	16	0.6	15.84
FN-FN	0.05	0.01	0	8	0	0.08
FP-FP	0.52	0.07	8	12	4.16	0.84
FP-TN	0.52	0.93	16	20	8.32	18.6
TN-FP	0.48	0.07	20	24	9.6	1.68
TN-TN	0.48	0.93	28	28	13.44	26.04

Furthermore, the edited payoffs have been added to the Gambit tool to obtain the game solution. If the detection efficiency of the local IDS is high, it sends a suspicious node statement to the global IDS, which in turn is accepted as a true statement. Therefore, the global IDS accepts the received statement and excludes the attacker or suspicious node from the network. On the other hand, the local IDS correctly detects the normal behavior of the node and sends the trust statement to the global IDS. Then, the global IDS accepts the normal behavior of the node based on the received trust statement from the local IDS. The solution of the game considering the detection efficiency rates of the local IDS and the main IDS is shown in the following figure (Figure 8).

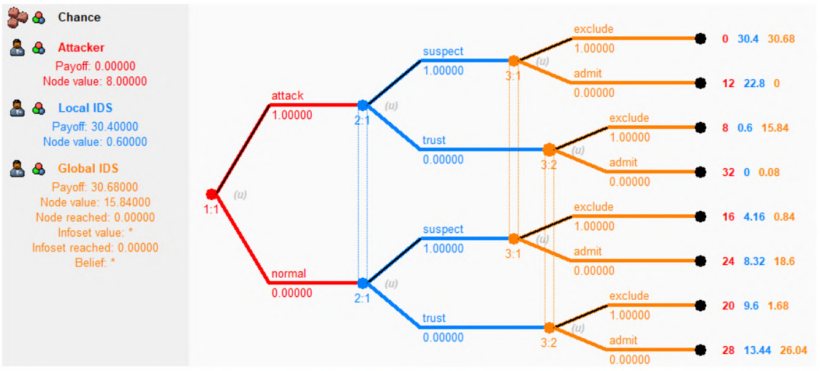

Figure 8. Solution of the game

Volume 1 (2026), Issue 2
pp. 69–85

TSARKA SCIENCE

eISSN: 3134-6057
pISSN: 3134-6049

In general, the decision-making of the main IDS depends mediately on the statement received from the local IDS. Despite the highly effective functionality of the global IDS, the full network security depends on the effectiveness of each local IDS in the network to detect an attack and prevent potential attacks. In such scenarios, game theory ensures secure communication in wireless networks, forming a security game can facilitate the process of reasoning actions and interconnection between different devices with limited resources. The existence of trust between nodes is a key component of network reliability and security mechanisms. Currently, the category of secure communication in wireless sensor networks faces problems arising from outsiders and insiders. Existing security schemes such as data encryption and authentication can only protect wireless sensor networks from outsider attacks. Several studies show the importance of a trust management scheme which is one of the effective approaches to detecting and protecting against insider attacks. The trust management system consists of five interrelated components: a collection of needed trust indicators, storage of received trust indicators, trust modeling, exchange of trust indicators, and decision-making [15,16].

1) Collection of the required confidence indicators. This component refers to

The collection of trust elements, which consists of the interaction status of the nodes obtained from each node. Confidence rating is evaluated based on this trust element.

2) Storage of trustworthiness scores obtained. This component of the trust management system considers the storage of information in a node consisting of the received trust rating data of neighboring nodes. However, the limited system resources of devices in wireless sensor networks must be considered when storing trust score data. And also, this data should be updated when new node rating data is obtained.

3) Confidence modeling. This component plays an important role in the design of a confidence management system. Confidence modeling consists of calculating the legitimacy of the received node confidence rating information.

4) Trustworthiness score exchange. This element of the trust management system represents the exchange of trust rating between two conventional nodes and transmission to the base station.

5) Decision-making. Based on the trustworthiness rating data received from the nodes, the base station system decides whether to add each node to the intermediate routing or exclude certain nodes from the network because of suspicious activities.

In wireless sensor networks, the existence of a trust mechanism is necessary to establish a secure connection between nodes [17]. In the trust and reliability mechanism, each node can assess the reliability of neighboring nodes by creating interactions between nodes. Trust and reliability mechanisms are based on the study of

TSARKA SCIENCE
Volume 1 (2026), Issue 2
pp. 69–85
eISSN: 3134-6057
pISSN: 3134-6049

interactions between different individuals, and in this context, game theory plays an important role in the design of a trust management system. IDS systems can perform the function of trust management between nodes by monitoring the behavior of nodes and storing information about the past properties of nodes to evaluate the reliability of each node [18,19]. Hence, based on the trust and reliability mechanism, a trust management system is established. The trust management system will be formed to strengthen the trust score of each node in the network and protect against insider attacks that can be launched by a compromised node. Meaning that the trust management system plays a key role in evaluating the quality of transmitted information, detecting anomalies, managing access control, and constructing the secure joint disposal of network resources.

4. Discussion

Game theory, with its foundation in economic and mathematical theory, provides a structured methodology to predict outcomes in competitive environments where the actions of each participant affect the others. Its application in WSNs represents a shift towards a more dynamic and predictive model of network security, where the focus is on understanding and anticipating the moves of potential attackers to devise effective defense strategies. This research aligns with prior studies that have highlighted the effectiveness of game theory in various fields, including cybersecurity, by facilitating a deeper understanding of adversarial behavior and enabling the formulation of strategic countermeasures.

One of the key findings from the simulations and theoretical models presented in this study is the concept of Nash Equilibrium, where no participant can gain by changing their strategy while the other participants keep theirs unchanged. This equilibrium concept is crucial in network security for designing strategies that ensure the stability of the network despite potential attacks. It enables network designers to anticipate vulnerabilities and adopt strategies that effectively mitigate the risks of attacks, thus enhancing the security and reliability of WSNs.

However, the application of game theory in network security is not without challenges. The assumption of rationality among network entities, which is a cornerstone of game theory, may not always hold in scenarios involving automated attacks or non-strategic adversaries. Moreover, the complexity of modeling and analyzing games increases significantly with the number of participants and possible strategies, which might limit the practical applicability of game-theoretic solutions in large-scale networks.

Despite these challenges, the potential benefits of applying game theory to network security are significant. It offers a proactive framework for security that goes beyond traditional reactive measures. Future research directions could include the development of sophisticated models that account for a broader range of attack scenari-

eISSN: 3134-6057
pISSN: 3134-6049

os, including those involving irrational behaviors, and the exploration of cooperative strategies for defense. Additionally, the integration of machine learning techniques could enhance the predictive capabilities of game-theoretic models, offering even more robust security solutions for wireless networks.

In conclusion, this study contributes to the growing body of knowledge on the application of game theory in network security, providing a novel perspective on the strategic interactions between network entities. By offering a framework for predictive and adaptive security measures, game theory represents a promising approach to safeguarding the integrity and functionality of wireless networks against the evolving landscape of cyber threats. Further research and development in this area are essential for realizing the full potential of game theory in enhancing network security.

5, Conclusion

A wireless network equipped with IoT devices is vulnerable to DoS attacks. In some cases, an attacker's goal may not be stealing sensitive data, but causing a denial of service to these systems. In the case of an intrusion by an outsider into a wireless network with resource-limited systems, an attacker can use one of the devices to perform DoS attacks using techniques like the transmission of large numbers of unnecessary packets to other systems. As a result, legitimate devices utilize their system resources while processing such unnecessary packets which leads to excessive consumption of power of these devices. Therefore, stable monitoring of the system's behavior in such networks using IDS technology plays a critical role in the maintenance of the secure network. Designing and managing the security of wireless networks is a non-trivial process, which involves a wide range of requirements for network responsiveness and quality [20,21]. Understanding the concept of security in wireless networks from a strategy and decision-making perspective can play an important role in improving security.

References

1. Ahmed, M. R. (2012). Wireless sensor network: Characteristics and architectures. https://publications.waset.org/9345/wireless-sensor-network-characteristics-and-architectures
2. Glushak, E. V., et al. (2023). Introduction to the Internet of Things (Vol. 1). Samara University Publishing House.
3. Olakanmi, O. O., & Dada, A. (2020). Wireless sensor networks (WSNs): Security and privacy issues and solutions. In Wireless mesh networks: Security, architectures and protocols (Vol. 13, pp. 1–16).
4. Cavalcanti, D., et al. (2019). Extending accurate time distribution and timeliness capabilities over the air to enable future wireless industrial automation systems. Proceedings of the IEEE, 107(6), 1132–1152.

TSARKA SCIENCE

Volume 1 (2026), Issue 2
pp. 69–85

eISSN: 3134-6057
pISSN: 3134-6049

5. Hussein, N. H., et al. (2022). A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions. IEEE Access, 10, 86127–86180.
6. Zahedi, F., & Farzaneh, N. (2020). An evolutionary game theory–based security model in vehicular ad hoc networks. International Journal of Communication Systems, 33(6), e4290.
7. Zenalabdin, H. S., Buhari, A., & Nyamasvisva, T. E. (2020). Performance analysis of IoT protocol stack over dense and sparse mote network using Cooja simulator. Journal of Physics: Conference Series, 1529(5), 052007.
8. Abughazaleh, N., Bin, R., & Btish, M. (2020). DoS attacks in IoT systems and proposed solutions. International Journal of Computer Applications, 176(33), 16–19.
9. Nishanth, N., & Mujeeb, A. (2021). Modeling and detection of flooding-based denial of service attacks in wireless ad hoc networks using uncertain reasoning. IEEE Transactions on Cognitive Communications and Networking, 7(3), 893–904.
10. D'Hondt, A., et al. (2015). RPL attacks framework. https://github.com/dhondta/rpl-attacks
11. Thomson, C., Romdhani, I., Al-Dubai, A. Y., & Wadhaj, I. (2016). Cooja simulator manual. ResearchGate. https://doi.org/10.13140/RG.2.1.4274.8408
12. Shi, H.-Y., Wang, W.-L., Kwok, N.-M., & Chen, S.-Y. (2012). Game theory for wireless sensor networks: A survey. Sensors, 12, 9055–9097. https://doi.org/10.3390/s120709055
13. Hoang, D. T., Lu, X., Niyato, D., Wang, P., Kim, D. I., & Han, Z. (2015). Applications of repeated games in wireless networks: A survey. IEEE Communications Surveys & Tutorials, 2102–2135. https://doi.org/10.1109/COMST.2015.2445789
14. Moustafa, N. (2019). The Bot-IoT dataset. IEEE Dataport. https://doi.org/10.21227/r7v2-x988
15. Fang, W., Cui, N., Chen, W., Zhang, W., & Chen, Y. (2022). A trust-based security system for data collecting in smart city. IEEE Transactions on Industrial Informatics.
16. Alam, S., et al. (2022). Trust management in social Internet of Things (SIoT): A survey. IEEE Access, 10, 108924–108954.
17. Dovgal, V. A., & Dovgal, D. V. (2021). Analysis of the problems of information security of wireless sensor networks and methods of ensuring the security of the Internet of Things. Vestnik of Adygeya State University. Series 4: Natural-Mathematical and Technical Sciences, 1(276), 75–83.
18. Korzhuk, V. M. (2019). Model and method for identification of network layer attacks on wireless sensor networks based on behavioural analysis (Dissertation abstract). St. Petersburg.
19. Legashev, L. V., et al. (2022). Development of a model for network traffic anomaly

detection in wireless distributed self-organising networks. Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics, 22(4), 699–707.

20. Ahmed, S., et al. (2021). Artificial intelligence and machine learning for ensuring security in smart cities. In Data-driven mining, learning and analytics for secured smart cities: Trends and advances (pp. 23–47). Springer.
21. Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. Sensors, 23(19), 8015.

Information about authors

Aknur Shahidani -
Department of Information Security
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan
e-mail: aknuraspring@outlook.com

Aigul Shaikhanova –
PhD, Professor, Department of Information Security
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan
e-mail: shaikhanova_ak@enu.kz
ORCID: https://orcid.org/0000-0001-6006-4813.

Gulvira Bekeshova -
Master of Technical Sciences
Senior Lecturer of the Department of Information Security
L.N. Gumilyov Eurasian National University
Astana, Kazakhstan
e-mail: bekeshova_gb@enu.kz
ORCID: 0000-0001-6006-4813

Lily Nurliana Abdullah -
PhD, Associate Professor, Department of Multimedia
Faculty of Computer Science and Information Technology
Serdang, Selangor, Malaysia
Universiti Putra Malaysia
e-mail: liyana@upm.edu.my
ORCID: https://orcid.org/0000-0001-8704-2390