International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

IMPROVING THE SECURITY OF WIRELESS SENSOR NETWORKS USING GAME THEORY

S.Thiravida Arasi
Research Scholar,
Department of Computer Science,
Adaikalamatha College,
(Affiliated to Bharathidasan University)
Vallam, Thanjavur, Tamil Nadu, India.

Dr.L.Nagarajan
Research Advisor, Director,
Department of Computer Science,
Adaikalamatha College,
(Affiliated to Bharathidasan University)
Vallam, Thanjavur, Tamil Nadu, India.

Abstract:

Wireless sensor networks are now widely used in a variety of applications. Wireless sensor networks are inherently unsecure and vulnerable to several forms of attacks because of how they are connected. This topic has been addressed in the past with a variety of techniques, each of which had drawbacks. Therefore, an effort was made to address these issues in the suggested solution. Game theory has also been utilised to more rapidly identify intrusive nodes in the proposed method for protecting sensor nodes, which is based on authentication based on the Interlock-enhanced ZKP protocol. Preventing assaults like sleep deprivation is one of the recommended solution's most significant advantages. The proposed technique was put into practise and evaluated in a MATLAB environment, and investigations revealed that the suggested approach performed really well.

Keywords: Wireless Sensor Networks, Authentication, Game Theory, Sleep Prevention Attack.

Introduction

This feature will make it feasible to utilise wireless sensor networks to monitor a range of surroundings utilising media and access control protocols (MAC). These, together with a broad variety of important protocols, are intended to cut down on energy uses. Wireless sensor network applications might call for safe, high-security settings due to their sensitive nature [1]. One of the most crucial and essential considerations when constructing wireless sensor networks is security and energy efficiency since sensors are frequently used to monitor sensitive situations [2]. The battery provides power for the sensor nodes [4] [5]. The sensor nodes cannot be recharged since they are situated in unique and inhospitable settings. The power and energy consumption of the nodes should be at a minimum due to the absence of maintenance and supervision of the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

existing nodes as well as their inability to recharge [5]. By turning off the transmitter and reception antenna and putting it to sleep, it is feasible to implement sensor consumption of the sensor nodes to the greatest extent possible. Energy and power use are reduced. According to the kind of communication required, MAC protocols alter sleep time dynamically [6] [7]. However, malevolent nodes may always penetrate the network and alter the node's sleep duration to shorten the node's lifespan using their knowledge of the MAC protocol. We refer to these attacks as sleep deprivation. In addition to examining the sleep inhibition attack in the wireless sensor network, the primary goal of this study is to provide a novel method for validating and authenticating hostile nodes that attempt to alter node sleep schedules. This feature will make it feasible to utilize wireless sensor networks to monitor a range of surroundings utilizing media and access control protocols (MAC). These, together with a broad variety of important protocols, are intended to cut down on energy uses. Wireless sensor network applications might call for safe, high-security settings due to their sensitive nature [1]. One of the most crucial and essential considerations when constructing wireless sensor networks is security and energy efficiency since sensors are frequently used to monitor sensitive situations [2]. The battery provides power for the sensor nodes [4] [5]. The sensor nodes cannot be recharged since they are situated in unique and inhospitable settings. The power and energy consumption of the nodes should be at a minimum due to the absence of maintenance and supervision of the existing nodes as well as their inability to recharge [5]. By turning off the transmitter and reception antenna and putting it to sleep, it is feasible to implement sensor consumption of the sensor nodes to the greatest extent possible. Energy and power use are reduced. According to the kind of communication required, MAC protocols alter sleep time dynamically [6] [7]. However, malevolent nodes may always penetrate the network and alter the node's sleep duration to shorten the node's lifespan using their knowledge of the MAC protocol. We refer to these attacks as sleep deprivation. In addition to examining the sleep inhibition attack in the wireless sensor network, the primary goal of this study is to provide a novel method for validating and authenticating hostile nodes that attempt to alter node sleep schedules.

Game theory is utilized in this strategy because it takes competing situations into consideration, and since these competitive factors are present in the detection of malicious nodes, it makes sense to seek for a solution that can both detect and perform well. In this proposed method, game theory was used to create these competitive and effective conditions and to produce much more useful results than other existing algorithms. In wireless sensor networks, the extracted decisions for nodes are also effective in the security of other nodes and do not only go back to the same node.

The linked principles are stated first in the following, followed by a review of earlier publications. The proposed approach is next described in detail, and finally, it is assessed. A basic overview is given towards the conclusion.

Game Theory

The following ideas are included in game theory. If the problem type is economic, then the following definitions apply to each of these terms: [8][13]

- The same economic elements are in competition with one another, player.
- Regulations: How to employ resources and opportunities as well as the game's rules.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600

http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

- Game Outcomes: The objectives that participants have for the game.
- Gain for players: The amount of profit made after factoring each player's popularity into the outcomes.
- Strategy: A detailed account of the choices the player takes in response to each occurrence.
- There are several varieties of game theory, such as:
- Asymmetric-asymmetric: A symmetric game is one in which the result of a strategy depends only on the other strategies that are utilised in the game, regardless of which player employs the approach [9].
- Zero-Total Non-Zero [9]: In a zero-sum game, the value of the game does not increase or decrease throughout the course of the game. In these games, one player's success is correlated with another's failure.
- Random-Non-Random [10]: While non-random games only use rational methods, random games include random aspects like rolling dice or dealing cards.
- Absolute Consciousness Full Consciousness [9]: Games with full consciousness allow all players to view the entire game board in front of them at all moment, like chess. The look and structure of the entire game is concealed from the players in games where they are not fully aware, such as card games.Strategy: A detailed account of the choices the player takes in response to each occurrence.
- There are several varieties of game theory, such as:
- Asymmetric-asymmetric: A symmetric game is one in which the result of a strategy depends only on the other strategies that are utilised in the game, regardless of which player employs the approach [9].
- Zero-Total Non-Zero [9]: In a zero-sum game, the value of the game does not increase or decrease throughout the course of the game. In these games, one player's success is correlated with another's failure.
- Random-Non-Random [10]: While non-random games only use rational methods, random games include random aspects like rolling dice or dealing cards.
- Absolute Consciousness Full Consciousness [9]: Games with full consciousness allow all players to view the entire game board in front of them at all moment, like chess. The look and structure of the entire game is concealed from the players in games where they are not fully aware, such as card games.Strategy: A detailed account of the choices the player takes in response to each occurrence.
- There are several varieties of game theory, such as:
- Asymmetric-asymmetric: A symmetric game is one in which the result of a strategy depends only on the other strategies that are utilised in the game, regardless of which player employs the approach [9].
- Zero-Total Non-Zero [9]: In a zero-sum game, the value of the game does not increase or decrease throughout the course of the game. In these games, one player's success is correlated with another's failure.
- Random-Non-Random [10]: While non-random games only use rational methods, random games include random aspects like rolling dice or dealing cards.
- Absolute Consciousness Full Consciousness [9]: Games with full consciousness allow all players to view the entire game board in front of them at all moment, like chess. The look and structure of the entire game is concealed from the players in games where they are not fully aware, such as card games.Strategy: A detailed account of the choices the player takes in response to each occurrence.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

- There are several varieties of game theory, such as:
- Asymmetric-asymmetric: A symmetric game is one in which the result of a strategy depends only on the other strategies that are utilised in the game, regardless of which player employs the approach [9].
- Zero-Total Non-Zero [9]: In a zero-sum game, the value of the game does not increase or decrease throughout the course of the game. In these games, one player's success is correlated with another's failure.
- Random-Non-Random [10]: While non-random games only use rational methods, random games include random aspects like rolling dice or dealing cards.
- Absolute Consciousness Full Consciousness [9]: Games with full consciousness allow all players to view the entire game board in front of them at all moment, like chess. The look and structure of the entire game is concealed from the players in games where they are not fully aware, such as card games.Strategy: A detailed account of the choices the player takes in response to each occurrence.
- There are several varieties of game theory, such as:
- Asymmetric-asymmetric: A symmetric game is one in which the result of a strategy depends only on the other strategies that are utilised in the game, regardless of which player employs the approach [9].
- Zero-Total Non-Zero [9]: In a zero-sum game, the value of the game does not increase or decrease throughout the course of the game. In these games, one player's success is correlated with another's failure.
- Random-Non-Random [10]: While non-random games only use rational methods, random games include random aspects like rolling dice or dealing cards.

- Absolute Consciousness Full Consciousness [9]: Games with full consciousness allow all players to view the entire game board in front of them at all moment, like chess. The look and structure of the entire game is concealed from the players in games where they are not fully aware, such as card games.Strategy: A detailed account of the choices the player takes in response to each occurrence.
- There are several varieties of game theory, such as:
- Asymmetric-asymmetric: A symmetric game is one in which the result of a strategy depends only on the other strategies that are utilised in the game, regardless of which player employs the approach [9].
- Zero-Total Non-Zero [9]: In a zero-sum game, the value of the game does not increase or decrease throughout the course of the game. In these games, one player's success is correlated with another's failure.
- Random-Non-Random [10]: While non-random games only use rational methods, random games include random aspects like rolling dice or dealing cards.
- Absolute Consciousness Full Consciousness [9]: Games with full consciousness allow all players to view the entire game board in front of them at all moment, like chess. The look and structure of the entire game is concealed from the players in games where they are not fully aware, such as card games.

Zero Knowledge Protocol

1. In cryptography, the (certifying) party can demonstrate to the (certifying) party that the assertion stated is true using the Zero Knowledge Protocol (ZKP). The assertion is exclusively verified using this approach, and no further information is sent other than confirmation that the statement is accurate

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

[12]. When it comes to math or even in real life, we frequently desire to explain things to others. For instance, if I believe that x is true and I want to persuade you that x is real, I will try to provide you with all the information I am aware of as well as the implicit conclusions that imply x is true. Proof P seeks to persuade V, the certifier, that his assertion is true. Typically, P provides V with some information in this regard, and V accepts the correctness of P's assertion by doing computations [14]. [15]. Can V be convinced without revealing sensitive information? Is it feasible to keep information while exchanging additional messages? Is it feasible to persuade V by conveying the information that is least valuable and taking into account the likelihood of a non-zero error? Bob must be persuaded by Alice that x is true, but only in a way that prevents Bob from learning anything else—that is, Bob gains no knowledge—in the process. For instance, while sending an email, the actions listed below are taken [16][17]:

2. Bob's public key is given to Alice by means of the business directory.
3. Using the public key, Alice communicates with Bob through encrypted messaging.
4. Bob now encrypts it using his private key.

Related Works

According to the discussion of game theory in reference [6], basic two-player games cannot examine complicated situations because of the significant dependency between players that emerges from problems like competitiveness, collaboration, and software and hardware communication. New games were thus released. These new games are referred to as dependent security games, where both malicious and non-malicious participants can alter the level of interest by adjusting the amount of security they spend. The most significant benefit of this research is its ability to ascertain each player's objective in these games, which is based on the level of investment made by other participants. The absence of risk quantification and evaluation, which should be taken into account in this form of assessment, is another shortcoming.

The authors of reference [7] offer a paradigm for risk management in the security industry. According to such perspective, a security-required organisation is divided into many components. For instance, a video service provider has five divisions: on-demand video service, network terminals, mobile television structures, and IT and support managers. They take into account vulnerability in each sector as well as budget and capital for security resources such that there is a linear link between them. They created two generic mathematical models based on linear dependencies; one is a multi-player model with an unrealistic game between portions, and the other is a model with a real game between them. The presentation of the risk model in the context of security is the research's most significant strength. It also has the drawback of having incomplete security needs organisation segmentation.

A network of users with competing goals is discussed in the reference [8]. The authors have presented a model in which network users invest in network security, or how much Internet users should pay to increase private and public security, in order to improve both their own personal security and the public security of the whole Internet. Their strategy views this situation as a non-cooperative multiplayer game and provides users with a number of functional sets depending on the defining of various security parameters. The authors offer a fair study of user tactics for each definition of network security level, such as total effort, weakest relationship, best hit, and

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

weakest aim. The research's decision to allocate resources to network security is one of its benefits and strengths.

The reference [9] discusses jamming games at the level of the wireless network access control environment, where each node in the network only knows the type of user it is (either a selfish user type or a malevolent user type). The authors saw this game as a two-player, multi-stage Bayesian game. The set of activities of a randomly accessible node are those transfer probabilities the node may choose from. The functional difference between the reward function (an ascending SINR function) and the energy price function represents the functional function of a self-centered user (an ascending function of node power). The difference between a malicious node's reward function and energy price function, whose reward function is zero if the other user is selfish and zero if the other user is a malicious node, defines the functional function of a malicious node. The model's incorporation of Bayesian equilibrium, which aids in achieving the predicted node strategies, is one of this study's merits.

The difficulties of network security against denial of service attacks are researched in the source [10]. To stop this kind of assault, the author has suggested a puzzle-based security strategy that may be distributed or not. A client asks a service from the service provider, the service provider selects a puzzle from the pool of riddles as a response to the customer, and lastly, if the solution is right, the provider provides resource service to the customer. This is how puzzle-based defence is characterised. The author of Distributed Attack has proposed a method to enhance the service provider's ideal defensive approach by modelling puzzle-based denial of service and defence as a two-player random game. Similar to an undistributed denial of service attack, a distributed denial of service attack on a system has the same fix.

In a wireless sensor network, the S-MAC protocol [18], which is used to synchronise sensor nodes, follows a predefined cycle that starts at compile time. Sending a SYNC message from one node to the next and back again is the activity of this cycle. As its name suggests, this message is used to synchronise network nodes. The SLEEP message is contained in every 11 bytes of SYNC bytes. The nodes are prepared to share data after delivering this message, and after doing so in unison, the activity enters the same sleep state. There is a connection that is outlined in Formula (1) and Fig. that governs how the nodes are moved into the Sleep state.

1, Shows the status of this protocol.

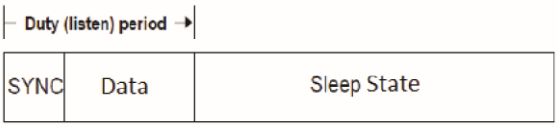

Fig. 1. A fixed cycle in S-MAC [18]

2. T-MAC protocol

Actually, this protocol is a better version of T-MAC. In this approach, all traffic is positioned at the start of the duty period to provide this improvement. Fig. 2 depicts the protocol's activity flow. The arrows in this diagram represent the messages that were sent and received. With the exception of having a Time Out mechanism, which is illustrated in the image with TA, this technique employs the same SYNC mechanism as the earlier protocol. If not invoked, this method puts the sleep node to sleep.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

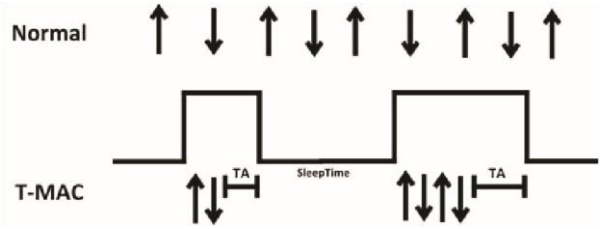

Fig. 2. A fixed cycle in T-MAC [19]

3. G-MAC protocol

The threshold values used in this algorithm serve the same purpose as those used in the first two techniques. Where GTIM stands for the same message sent to the Gateway and RTS stands for the same request to transmit to the Gateway [20]. This protocol places a lot of emphasis on the Gateway phase, where information is sent both inside a cluster and to the Gateway.

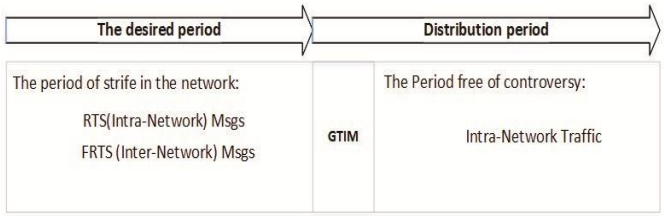

Fig. 3. G-MAC Protocol [20]

Proposed Method

Here, a simulation using the SMAC protocol is used to show how a sleep apnea attack works. The SLA protocol is utilized to identify a sleep apnea attack in all four cases of implementation when there is zero knowledge. In this case, keys are exchanged using the Hashing and Interlock protocols, and the base station is verified using the Zero Knowledge Protocol (ZKP). This method's application of game theory is structured so that the nodes act as players and that delivering messages based on viewpoints constitutes a movement in the game. If the authentication mechanism for transmitting packets is incorrect, the player or node loses one point. If the score falls below the cutoff, the attacking node is indicated, allowing for the identification of unknown and potentially harmful nodes. The algorithm's use and location determine the threshold value. In military applications, for instance, the value of this threshold may be one, meaning that the node is ignored after the first authentication failure, even though, for instance, there might be an issue with the node at that very moment. The node is not regarded as an attack node, but rather as a threshold in security applications when safety is crucial and the risk is extremely high. This may also be the case in other applications, such as fire detection nodes. Because the danger in these applications might be larger, the threshold shifts to higher values in the forest. As a result, it is clear that in this situation, nodes cannot be given more chances for authentication and are excluded after making their first mistake.

A crucial procedure involves moving the keys from the base station to other nodes, and these keys are always vulnerable to assault from the general public. The keys are sent via the Interlock protocol, which encrypts each key with the AES algorithm to prevent them from a common attack. The Interlock protocol divides the key encryption process into two pieces. The first portion is communicated simultaneously, and the second part is transmitted upon receipt of a response from the receiving node. The receiving base station may only decrypt the key by linking these two parts. Each network's connection nodes must agree on a variety of key symmetric encryption strategies in order to carry out this transfer. The AES algorithm is used in this suggested technique. By using this technique, the encryption process is split into two steps. After the initial transfer has been authenticated by legitimate nodes, these two portions are transferred one after the other. In sensor networks, MAC protocols are used to modify node sleep

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

times. Asynchronous signals are sent by MAC protocols to control the nodes' sleep time. Request control (RTS) and ready to send (CTS) signals are sent to make this protocol (MAC) function. Synced packets are used with these two signals (SYNC). Responding to control packets like RTS messages can help avoid sleep deprivation. The nodes' energy is substantially squandered since they can't sleep because they are constantly responding to control packets. The network nodes won't have enough time to fall to sleep and restore to their initial states if these control messages are transmitted often. The nodes' battery life decreases as a result of this. All nodes in the attacker node's field lose energy at this point. The SYNC message is sent by the attacker. This demonstrates to the nodes that the node goes to sleep after transmitting. In order to keep synchronisation, each node that gets a SYNC packet within the same period or sleep time recalculates its subsequent sleep time. As nodes in sensor networks find it difficult to quickly zero the time before sleep, the received SYNC packet's time value is determined as follows:

Receiving a SYNC packet does not modify your sleep schedule while using this approach. In other words, using this strategy simultaneously enables the nodes to steadily enhance their synchronisation. In reaction to receiving SYNC packets, the sleep deprivation assault might be launched. An attack node that tracks network traffic can easily recognize these packets even if they are encrypted. In other words, the attack node enables the identification of all packets by the measurement of their size and duration. For instance, S-MAC SYNC packets are about 10-B long and sent out a few moments after the S-MAC frame starts. Even if it is encrypted, an attacker node merely alters packets and discovers this information once and for all. To defend the network from these assaults, we utilize authentication protocols in the suggested approach.

The proposed design's flowchart is shown in Fig. 4. Each research evaluates the suggested system using a number of parameters.

To construct the sensor nodes in the network and to authenticate them, the proposed technique generates a public key and a private key for their communication. To do this, we create the key using the RSA technique. The interlock protocol is used to exchange keys in order to safeguard the connection between nodes against common attack, as seen in the figure above (MITM). Fig. 4 depicts the suggested system design. The base station (BS) in the suggested design has access to data from all sensor nodes, including headers and nodes that are managed by it. The base station in the negotiation appears as a third party once the nodes have been verified. The receiving node now serves as the message authenticator, while the sleep sync message node serves as the receiver. Each node has a private key, known in this system as the S key, according to the suggested flowchart in Fig. 4. Here, certifiers and public key suppliers collaborate. The base station transmits the genuine secret key when the authenticator requests it during the authentication procedure.

In the suggested technique, the base station calculates the value of the expression in Equation (3) rather than transmitting the secret key directly.

$$V\ S^2 = \mathrm{mod} N \qquad (3)$$

S is the private key and N is the public key in Equation (3). For each authentication request made in this case, a value of V is processed. The zero knowledge protocol makes it impossible to predict random integers when it is used for authentication. The likelihood of an authentication mistake is consistently lowered by up to 50% by

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

using the zero knowledge protocol. Here, the proof's private key S is still a mystery. This makes it challenging to get S from Equation (3).

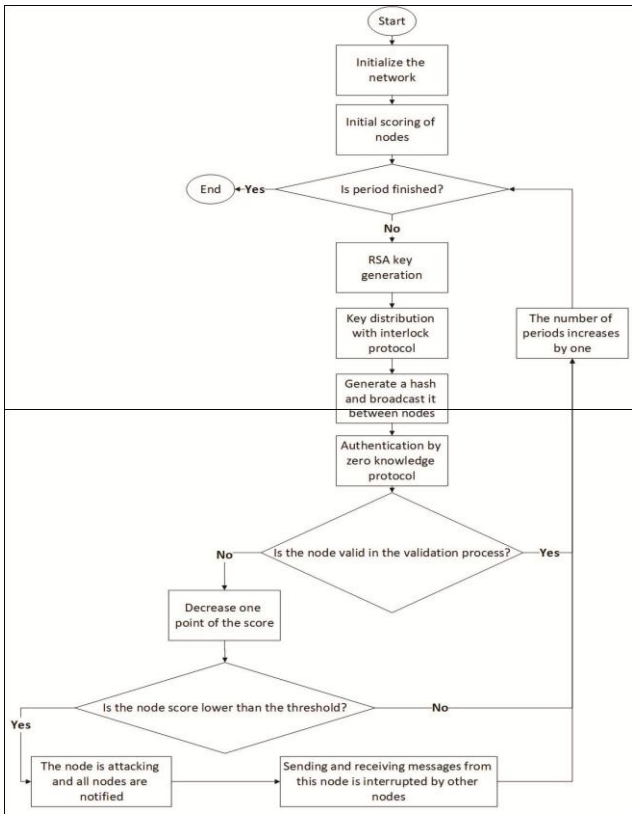

Fig. 4. Proposed workflow diagram

- Identify an attack in the suggested approach.
- The following steps are required to carry out this algorithm in the suggested system (in this proposed algorithm, nodes are viewed as game pieces in game theory and transmitting messages as a movement in the game):
- The RSA algorithm is used by the base station to create public keys.
- Interlock is a mechanism that is used to distribute these keys across nodes.
- In the suggested technique, the sending node serves as the proverb and the receiving node serves as the message authenticator.
- A private key, referred to in this system as the S key, exists on each node.
- Here, certifiers and public key suppliers collaborate.
- The proof node creates v and hashes it using relation while keeping the public key, the private key, and (3). In a sense, it can be claimed that this produced key is identical to the secret key of the associated node, and it is clear that in this situation, there is a very low possibility that the key can be found.
- The secret key of the receiving node is sought from the base station on the confirmation node side, where this message was received, so that the authentication node can carry out authentication.
- If the authentication node compares the values received from the base station and the proof node and finds that they match, the authentication will be successful and the node's score won't be affected. If not, the authentication won't be successful and the node's score will be affected. The proposed method can detect this kind of attack with very little overhead if the score of the proving node drops below the threshold, identifying it as the attacking node. As a result, all messages received from the attacking node are then passed by the acknowledging node, resulting in the DoS attack failing here.

EVALUATION

To simulate the application, R2017b 64-bit of the MATLAB programming language was utilised. Numerous application capabilities are easily accessible thanks to this programme. The suggested method was emulated on a machine with the hardware requirements listed in

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

Table I

Simulator System Hardware Specifications

Item	Value
Processor	Intel(R) Core(TM) i7-5500 CPU, 2.40 GHz 2.40GHz
Installed memory (RAM)	8.00 GB
Display Adaptor	ATI Radeon HD 5570, 2048 MB
System type	64-bit
Operating Systems	Windows 10 Enterprise
Hard	1TB

We must first specify the number of nodes in our simulation. The SMAC protocol is used by nodes to update sleep time. The nodes were routed using the AODV protocol during the simulation. The anticipated simulation time is 50 milliseconds. Each node's starting energy in this simulation is set at 1000 mW. In this simulation, a wireless channel is being used. As the MAC protocol, SMAC is employed. It uses 0.014 mW while it is not in use and 0.036 mW when it is transmitting. Additionally, the energy consumption for dormant nodes is 0.000015 mW. 0.028 MW of energy is needed to change from one state to another. The base station in this scenario creates the keys using the RSA method. The simulation's data parameters are as shown in Table II.

TABLE II

Simulator System Hardware Specifications

Parameter	Value
Number of attacking nodes	1
Ambient size	50 * 50
Total number of nodes	100
Number of base stations	1
Number of packages sent	2
Energy required when idle and receiving	0.014
Energy required to send	0.036
Energy consumption in sleep mode	0.000015
change the mode	0.028

The graphs in this part show the simulation time on the x-axis, battery energy on the y-axis, packet delivery rate on the z-axis, and output power on the output power axis. The attacks that are tried to be stopped here are DoS attacks.

The quantity of battery power utilised during the simulation is depicted in Fig. 5. As can be observed, a DoS attack causes a significant reduction in grid energy, which results in nodes dying before they should. Here, the energy of the nodes is clearly dropping, and this is shown by the use of the colour red. The zero knowledge protocol for SYNC message transmitting nodes is used here to stop the assault. It can be observed how the energy is lowered in the red graphic, which generally depicts a situation in which the destructive node has not been located. The blue graphic demonstrates how the sensor network's lifespan is greatly increased by shielding the nodes from attack. The graph produced shows that the suggested technique is poorer than usual and consumes more energy, but from a point of view.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

This is because the multi-stage authentication used in the proposed method of this research uses a little bit more energy than usual. The energy consumption of the nodes becomes ideal and normal in the suggested technique when the destructive node is found, yet it still decreases in the red plot. The network under examination in this scenario vanishes significantly more quickly than the network for the suggested strategy. The suggested approach will undoubtedly last longer and, because it makes use of game theory, can detect malicious nodes with a lot less effort.

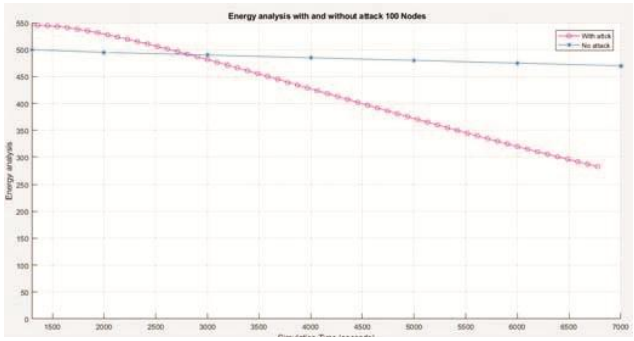

Fig. 5. The amount of battery energy used during the simulation

By contrasting the packet delivery rates under assault and without attack in the figure in Fig. 6, we demonstrate how the performance of the sensor network is enhanced when attacks are prevented. The attack scenario depicted in the red graph is one in which the attacking node repeatedly plays packets, which causes the packet delivery rate to decline sharply once the node battery is exhausted, as shown in the preceding diagram. Due to the processes necessary to authenticate and identify rogue nodes, the proposed method's package delivery rate initially performs poorly. Because authentication is performed first in the proposed solution of this research and after identification, each time authentication is performed, we can say that there is only one initial overhead in the proposed method. However, after the malicious nodes are identified and authentication is performed for all nodes, the packet length rate increases.

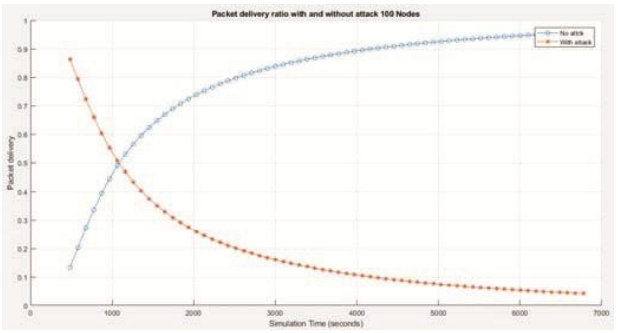

Fig. 6. Package delivery rate in attack mode and without attack

As the attack is stopped in Fig. 7, the output power increases. The sensor network's output power is increased in the event of an attack prevention. The attack scenario is depicted in the red graphic and is mitigated by the attacker node repeatedly distributing packets after the node battery has been depleted.

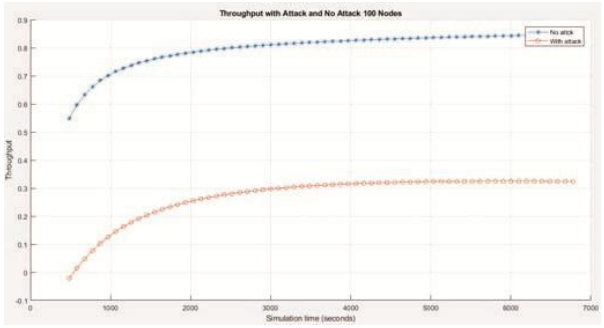

Fig. 7. Output in attack mode and without attack

In a sense, it can be claimed that in this situation, the overhead will diminish the operational power and lead to inferior network performance, as can be seen in Fig. 8 average waiting time in a typical network, which shows

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

how waiting times are affected over time by destructive nodes that are already there. There was evidence of an assault. Naturally, the suggested technique does not include this waiting period since hostile nodes are rapidly identified in this study proposal; hence, there is no waiting period caused by the existence of malicious nodes in this scenario. In the network of the suggested technique, nodes are not transferred in order to lengthen the waiting time.

In a sense, it can be claimed that in this situation, the overhead will diminish the operational power and lead to inferior network performance, as can be seen in Fig. 8 average waiting time in a typical network, which shows how waiting times are affected over time by destructive nodes that are already there. There was evidence of an assault. Naturally, the suggested technique does not include this waiting period since hostile nodes are rapidly identified in this study proposal; hence, there is no waiting period caused by the existence of malicious nodes in this scenario. In the network of the suggested technique, nodes are not transferred in order to lengthen the waiting time.

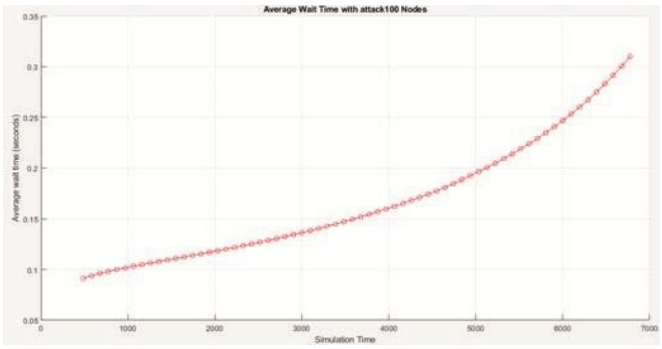

Fig.8. The average waiting time on a typical network despite an attack

Fig. 9 shows the error rate during simulation for the recommended technique versus the standard scenario. In the conventional scenario, the error rate increases continuously, but in the recommended method, it is zero. This is feasible because there is a technique that, if the node is authorised, transmits the package without sending any error signals. The proposed protocol cannot provide sufficient authentication of the destructive node.

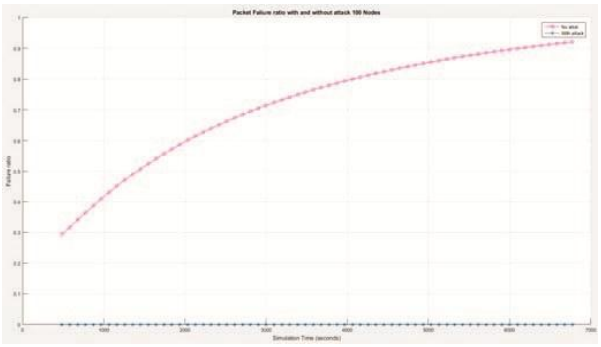

Fig. 9. Closed error rate in a typical network despite the attack and the proposed method

The results of the proposed study are contrasted with those of the Zhang approach [21], Ranjeetha approach [22], Tao approach[23], and Turki Approach[24], as shown in Fig. 10. The several techniques for protecting WSNs include these.

Fig. 10 shows the total number of packets transmitted by the receiver as well as the rate of packet loss.

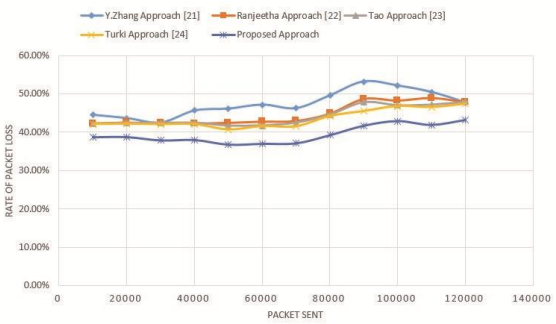

Fig. 10. Packet Sent vs Rate of Packet Loss

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

As can be observed, the suggested approach is able to have a lower Rate of Packet Loss than previous techniques; this is an indication of the proposed method's superior security and accuracy.

Conclusion

The innovative method for validating and authenticating hostile nodes that attempt to alter nodes' sleep schedules is suggested in this dissertation. The suggested method for validating and authenticating sensor nodes that communicate sleep synchronisation messages is based on the zero-knowledge protocol and game theory. The suggested solution involved exchanging keys using the Interlock protocol to boost security. All nodes that transmit SYNC messages are verified in the suggested approach before the message is accepted or refused. As a result, the suggested approach works well to stop attacks caused by sleep deprivation. The attacker node cannot spread the sleep synchronisation signal in the proposed manner since it is unacceptable to allow sleep time without authentication. Sensor network nodes only have a few resources and skills. Most significantly, excessive network resource utilisation may shorten the life of the network. In order to avoid sleep deprivation, the suggested technique makes use of the authentication mechanism of nodes that attempt to deliver SYNC packets. The protocol for zero knowledge is used for this. The simulation findings demonstrate that the network life is increased by stopping the assault. Although the network has secure connections, this protection mechanism also makes the network last longer. In other words, the security architecture proposed in this paper offers a complete security remedy for vulnerabilities. The suggested method uses less network resources and is an appropriate security strategy for wireless sensor networks since it combines the zero-knowledge protocol with the interlock protocol for key transfer to secure the packages from common attacks.

One idea that may be made is to offer a method for trustworthy clustering that enables the detection of malicious nodes inside clusters and takes into account both conventional clusters and virtual clusters using game theory. Assign the nodes to these two clusters, i.e., the nodes with the correct score are added to the list of real clusters at the start, and the nodes whose score is low for a variety of reasons are added to the list of virtual clusters and the nodes that are in the list of virtual cluster nodes. They cannot be transmitted or received, which increases the security of sending and receiving items.

References

1. Game Theory and Wireless Sensor Networks: An Overview, C. Comaniciu and M. Manic, 2012.
2. Introduction to Game Theory and Its Applications in Wireless Sensor Networks, P. S. Pathak, 2016.
3. Game Theory in Wireless Sensor Networks: A Survey, A. Rahman, M. A. Sattar, and M. A. Imran, 2015.
4. Game Theory in Wireless Sensor Networks: Recent Advances, M. D. Sanadhya, K. J. Ravi, and T. R. Reddy, 2014.
5. Game Theory in Wireless Sensor Networks: A Comprehensive Survey, P. Wang and X. Yang, 2013.
6. Game Theory in Wireless Sensor Networks: A Tutorial, S. S. Iyengar, 2009.
7. Recent Developments in Wireless Sensor Networks: A Game Theory Perspective, A. Anpalagan and E. H. Geraniotis, 2009.
8. Osadchy, M., & Panait, L. (2008). Wireless sensor networks and game theory.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 11, Issue 1, No 2, 2023. ISSN: 2348-6600
Reference ID: IJCS-464 PAGE NO: 3151-3164

International Journal of Computer Science and Network Security, 8(3), 58-63.
9. Shanmugam, K., & Jesudasan, S. (2010). Game theory and its application in wireless sensor networks. International Journal of Computer Science and Network Security, 10(4), 43-51.
10. Li, M., & Li, Y. (2010). Game theory for wireless sensor network: An overview. International Journal of Ad Hoc and Ubiquitous Computing, 4(2), 104-110.
11. Paruchuri, V., & Mishra, S. (2015). A survey on game theory based models in wireless sensor networks. Ad Hoc & Sensor Wireless Networks, 25(1), 1-24.
12. Chai, Y., & You, X. (2006). Game theory in wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials, 8(2), 34-4