JACET

J. ADV COMP ENG TECHNOL, 7(2) Spring 2021

Improving the Security of Wireless Sensor Networks Using Game Theory

Behzad Seif[1], Mohammad Goodarzi[2]
1- Department of Computer Engineering, Garmsar branch, Islamic Azad University, Garmsar, IRAN.
2- Department of Computer Engineering, Garmsar branch, Islamic Azad University, Garmsar, IRAN.
(m_goodarzi181@yahoo.com).

Received (2021-02-22) Accepted (2021-10-09)

Abstract: *IToday, the use of wireless sensor networks has become very popular in many applications. Due to the connection in wireless sensor networks, it is done wirelessly, so they are naturally insecure and prone to various types of attacks. In the past, various solutions were offered in this regard, each of which had its problems. Therefore, in this proposed solution, an attempt was made to solve these problems. The proposed solution for securing sensor nodes uses authentication based on the ZKP protocol, which has been improved with Interlock, and game theory has also been used to more quickly identify intrusive nodes. One of the most important benefits of the proposed solution is to prevent attacks such as sleep deprivation. The proposed solution was implemented and reviewed in MATLAB environment and the studies showed a very good performance of the proposed method.*

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

How to cite this article:
Behzad Seif, Mohammad Goodarzi. Improving the Security of Wireless Sensor Networks Using Game Theory. J. ADV COMP ENG TECHNOL, 7(2) Spring 2021 : 93-102

I. INTRODUCTION

Wireless sensor networks can be used to monitor a variety of environments and thus have a wide range of significant applications. Applications that use wireless sensor networks are sensitive in nature and may require secure, high-security environments [1]. Since sensors are commonly used to monitor sensitive environments, considering security and energy efficiency is one of the most important and necessary issues when designing wireless sensor networks [2]. Sensor nodes draw their energy from the battery [4] [5]. Because the sensor nodes are located in special and inaccessible environments, it will not be possible to recharge them. Due to the lack of care and monitoring of the established nodes as well as the inability to recharge, the power and energy consumption of the nodes should be optimal [5]. To implement sensor networks with optimal or minimal energy consumption, the nodes are periodically switched off and dormant [4]. Implementation of this feature will be possible using Media Access Control Protocols (MAC). These protocols are designed to reduce the energy consumption of the sensor nodes as much as possible by disabling the transmitter / receiver antenna and bringing it to sleep. This saves energy and electricity consumption. MAC protocols change sleep time dynamically based on the type of communication required [6] [7]. However, malicious nodes can always infiltrate the network and use their information about the MAC protocol to manipulate the node's sleep time to reduce the node's lifespan. This type of attack is called sleep deprivation. The main purpose of this study, in addition to investigating the sleep inhibition attack in the wireless sensor network, is to propose a new scheme for validation and authentication of malicious nodes that are trying to change the

sleep schedule of nodes.

In this proposed method, game theory is used because game theory considers competitive conditions and in the detection of malicious nodes, these competitive conditions exist exactly, so we should look for a solution that can detect and have a good performance. In security of wireless sensor networks the extracted decisions for nodes are also effective in the security of other nodes and not only goes back to the same node, so in this proposed method, game theory was used that can create these competitive and effective conditions and To produce much more useful results than other present algorithms.

In the following, first the related concepts are expressed and then a review of previous works is done. Then the proposed method is stated in all its details and then the proposed method is evaluated. At the end, a general summary is stated.

II. GAME THEORY

There are the following concepts in game theory. If we consider the type of problem as economic, then the definition of each of these concepts is [8][13]:

- Player: The same economic factors are competing with each other.
- Rules: How to use opportunities and resources as well as the rules governing the game.
- Game Outcomes: What players aim for after the game.
- Benefit of players: The amount of profit obtained by putting the results in the function of the desirability of each player.
- Strategy: A complete description of the decisions that the player makes under each event.
- There are different types of game theory, including:
- Asymmetric-asymmetric: A symmetric game is a game in which the outcome of a strategy depends solely on what other strategies are used in the game [9], and is independent of which player adopts the strategy.
- Zero-Total Non-Zero [9]: Zero-sum games are games in which the value of the game remains constant during the game and does not decrease or decrease. In these games, the profit of one player is associated with the loss of another player.
- Random-Non-Random [10]: Random games contain random elements such as rolling dice or handing out cards, and non-random games are games that have purely logical strategies.
- Full Consciousness-Without Full Consciousness [9]: Full conscious games are games in which all players can see the entire composition of the game in front of them at any time, such as chess. On the other hand, in games without full awareness, the appearance and composition of the whole game is hidden for the players, such as games that are played with cards.

III. ZERO KNOWLEDGE PROTOCOL

The Zero Knowledge Protocol (ZKP) in cryptography is the way in which the (certifying) party can prove to the (certifying) party that the statement made is correct. This method only verifies the statement and does not send any additional information other than the fact that the statement is actually true [12]. We usually want to explain things to others in math or even in real life. For example, I know x is true, and if I want to convince you that x is true, I will try to tell you all the facts I know, as well as the implicit results that show x is true. Proof P tries to convince certifier V that his claim is correct. Normally, P gives some information to V in this connection and V accepts the accuracy of P's claim by performing calculations [14] [15]. Can V be persuaded without transferring important information? Is it possible to exchange more messages while retaining information? Is it possible to convince V by considering the probability of non-zero error and by transferring the least useful information? Alice has to convince Bob that x is true, but so that Bob cannot get any information other than the process of convincing Alice; That is, Bob acquires zero knowledge. For example, in email, the following steps are performed [16][17]:

1. Alice receives Bob's public key from the company directory.
2. Alice sends an encrypted message to Bob with the public key.
3. Bob now uses his secret key to encrypt it.

IV. RELATED WORKS

In reference [6], game theory is discussed and

it is said that due to the high interdependence between players that results from issues such as competition, cooperation and software and hardware communication, simple two-player games are not able to analyze complex situations. So new games were introduced. These new games are known as dependent security games in which there are several malicious and non-malicious players who increase or decrease the interest by changing the amount of their security investment. The most important strength of this research is to determine the goal of each player in these games, which depends on the amount of investment of other players. Also one of the weaknesses is the lack of risk assessment and estimation that should be considered in this type of assessment.

In reference [7], the authors provide a model for risk management in the field of security. In that view, an organization in need of security is considered to consist of several parts. For example, a video service company consists of five divisions: core networks, mobile structures for television, network terminals, IT and support managers, and on-demand video service. In each sector, they consider security resources as budget and capital so that there is a linear relationship between them, as well as vulnerability in each sector. Based on linear dependencies, they developed two general mathematical models, one is a multi-player model with impractical game between sections, and the other is a practical game model between them. The most important strength presented in this research is the presentation of the risk model in the field of security. It also has the disadvantage that the segmentation of the security needs organization was not complete.

In the reference [8], several users in a network are considered with conflicting goals. In order to improve their private security and the public security of the entire Internet, the authors have proposed a model in which network users invest in network security, that is, how much Internet users should spend to improve private and public security. Their approach sees this scenario as a non-cooperative multiplayer game and offers users several sets of functional functions based on the definition of different values of security. For each definition of network security level, such as total effort, weakest relationship, best hit, and weakest goal, the authors provide a balanced analysis of user strategies. One of the advantages and strengths of this research is the allocation of capital network to network security.

In the reference [9], in relation to jamming games at the level of the wireless network access control environment, while each node in that network knows only its type (selfish user type or malicious user type), Is discussed. The authors have considered this game as a multi-stage Bayesian game with two players. The set of transfer probabilities that a randomly accessible node can select is considered as the set of activities of that node. The functional function of a selfish user is the difference between the reward function (an ascending SINR function) and the energy price function (an ascending function of node power). The functional function of a malicious node is the difference between its reward function and its energy price function, whose reward function is zero if the other user is selfish, and zero if the other user is a malicious node. One of the strengths of this research is the use of Bayesian equilibrium in the model, which helps to achieve the expected strategies of the nodes.

In the reference [10], the problems of defense against denial of service attacks in the network are studied. The author has proposed a puzzle-based defense solution that can be distributed or non-distributed to counter this type of attack. Puzzle-based defense is described as follows: first, a customer requests from the service provider, then, the service provider responds to a puzzle from the pool of puzzles as a response to the customer, and finally, if the answer is correct, the provider Provides resource service to the customer. The author of Distributed Attack has modeled puzzle-based denial of service and defense as a two-player random game, and has suggested a way to improve the service provider's optimal defense strategy. The solution to a distributed denial of service attack on a system is based on the same solution as an undistributed denial of service attack.

1. S-MAC protocol

The S-MAC protocol [18], which is used to synchronize sensor nodes, goes through a fixed cycle in a wireless sensor network that begins at compile time. The activity in this cycle is to send a SYNC message from one node to another and from there to the next node. This message, as its name implies, is used to synchronize between

network nodes. Each 11 bytes of the SYNC message also contains 2 bytes of the SLEEP message. After sending this message, the nodes are ready to exchange data, and after doing so in sync, the activity is in the same sleep mode. How the nodes are transferred to the Sleep state follows a relation that is specified in Formula (1) and Fig. 1, shows the status of this protocol.

$$SleepTime = [\frac{SleepTime + SYNC.SleepTime}{2}] \quad [18](1)$$

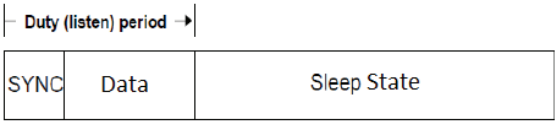

Fig. 1. A fixed cycle in S-MAC [18]

2. T-MAC protocol

This protocol is actually an improved model of T-MAC. In this model, to create this improvement, all traffic is placed at the beginning of the duty period. Fig. 2 shows the process of activity in this protocol. In this figure, the directions indicate the messages sent and received. This method uses the same SYNC mechanism, except that it has an advantage over the previous protocol in that it also has a Time Out mechanism, which is shown in the figure with TA. This mechanism causes the sleep node to go to sleep if not used.

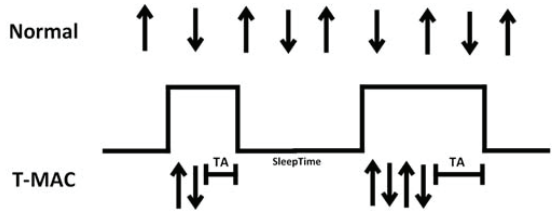

Fig. 2. A fixed cycle in T-MAC [19]

3. G-MAC protocol

The main focus of this protocol is on the Gateway section, where data is exchanged within a cluster as well as towards the Gateway; But this algorithm, like the previous two methods, has threshold values that have the same function; Where RTS is the same request to send to the Gateway and GTIM is the same message that is sent to the Gateway [20].

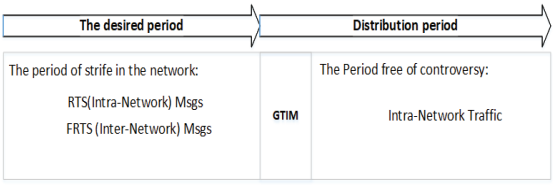

Fig. 3. G-MAC Protocol [20]

V. PROPOSED METHOD

Here, a scenario is implemented on the SMAC protocol to demonstrate the mechanism of sleep apnea attack. Implemented attack there is zero knowledge in all four instances of execution, and the SLA protocol is used to detect a sleep apnea attack. In this scenario, Hashing and the Interlock protocol are used to exchange keys, and the Zero Knowledge Protocol (ZKP) is used to authenticate the base station. In this proposed method, game theory is used and the method of use is such that the nodes are as players and sending depending on the perspective is a movement in the game. If the authentication mode for sending packets is not done correctly, one point is deducted from the player or the node, and if the score is below the threshold, it means the attacking node, and thus unknown and dangerous nodes can be identified. The threshold value depends on how the algorithm is used and where it is used. For example, in military applications, the value of this threshold can be one, which means that the node is left out with the first authentication error, while for example there may be a problem with the node at that moment. And the node is not considered as an attack node, but in security applications where security is very important and the risk in these applications is very dangerous, it is done in this way and is considered a threshold, but may be in other applications such as fire detection nodes. In the forest this threshold changes to higher values because in these applications the risk can be higher and therefore it can be seen that in this case the nodes cannot be given other opportunities for authentication and with the first error by the node, the node is left out.

Moving the keys from the base station to other nodes is a vital process, and these keys can be attacked by the public at any time. To protect the keys against a popular attack, the keys are transferred by the Interlock protocol, in which

each key is encrypted using the AES algorithm. In the Interlock protocol, the key encryption process is divided into two parts, the first part is transmitted at the same time, while the second part is transmitted after receiving a response from the receiving node, only by connecting these two parts, the key can be decrypted at the receiving base station. To perform this transfer, link nodes on each network must agree on a number of key-symmetric encryption techniques. This proposed method uses the AES algorithm. This algorithm divides the encryption process into two parts. These two sections are sent one after the other with the authentication of the first transfer by valid nodes. In sensor networks, the sleep period of nodes is adjusted using MAC protocols. MAC protocols regulate the sleep period of nodes by sending synchronous signals. This protocol (MAC) works by sending request control (RTS) and ready to send (CTS) signals. These two signals are used as synchronous packets (SYNC). An effective way to prevent sleep deprivation is to respond to control packets such as RTS messages. Responding to control packets prevents the nodes from sleeping and as a result the nodes' energy is severely wasted. If these control packets are sent at short intervals, then the nodes in the network do not have enough time to go to sleep and return to the original state. This causes the nodes to lose battery power. Here all nodes within the range of the attacking node lose their energy. The attacker sends the SYNC message. By doing this, it shows the nodes that after sending, the node goes to sleep. Each time one node receives a SYNC packet from another node in the same period or sleep time, that node recalculates its next sleep time to maintain synchronization. In sensor networks, nodes do not easily zero the next sleep time, and the amount of time in the received SYNC packet is calculated as follows:

$$NewSleepTime = \frac{OldSleepTime + \mathrm{Re}ceiveSYNCpkt.SleepTime}{2} \quad (2)$$

This method does not effectively change sleep time when receiving a SYNC package. In other words, this method at the same time allows the nodes to gradually improve synchronization over time. The sleep deprivation attack can be executed in response to SYNC packets. Even if these packets are encrypted, an attack node that monitors network traffic can easily identify these packets. In other words, the attack node makes it possible to identify all packets by examining their size and time. For example, S-MAC SYNC packets are approximately 10-B long and are performed within a few milliseconds of the beginning of the S-MAC frame. An attacker node detects this information once and for all, even if it is encrypted, easily modifies packets. Accordingly, in the proposed method, we use authentication protocols to protect the network against these attacks.

Fig. 4 describes the flowchart overview of the proposed design. In each research, a series of parameters are evaluated to evaluate the proposed system.

In this proposed scheme, a public key and a private key are generated for the communication of the sensor nodes in order to establish the nodes in the network and to authenticate them. To do this, we use the RSA algorithm to generate the key. According to the diagram above, the keys are exchanged using the interlock protocol to protect the connection of nodes against popular attack (MITM). The proposed system architecture is shown in Fig. 4. In the proposed architecture, the base station (BS) has access to the information of all sensor nodes, such as the headers and the nodes under its management. When the nodes are authenticated, the base station in the negotiation appears as a third party. The sleep sync message node now acts as the receiver and the receiving node acts as the message authenticator. According to the proposed flowchart in Fig. 4, each node has a private key, which in this method is known as the S key. Here the public key providers and certifiers share. When, in the authentication process, the secret key is requested by the authenticator, the base station sends the authentic secret key.

In the proposed method, instead of passing the secret key directly, the value of the expression in Equation (3) is calculated by the base station.

$$V = S^2 \bmod N \quad (3)$$

In Equation (3), S is the private key and N is the public key. Here a value of V is processed for each authentication request. Now, when the zero

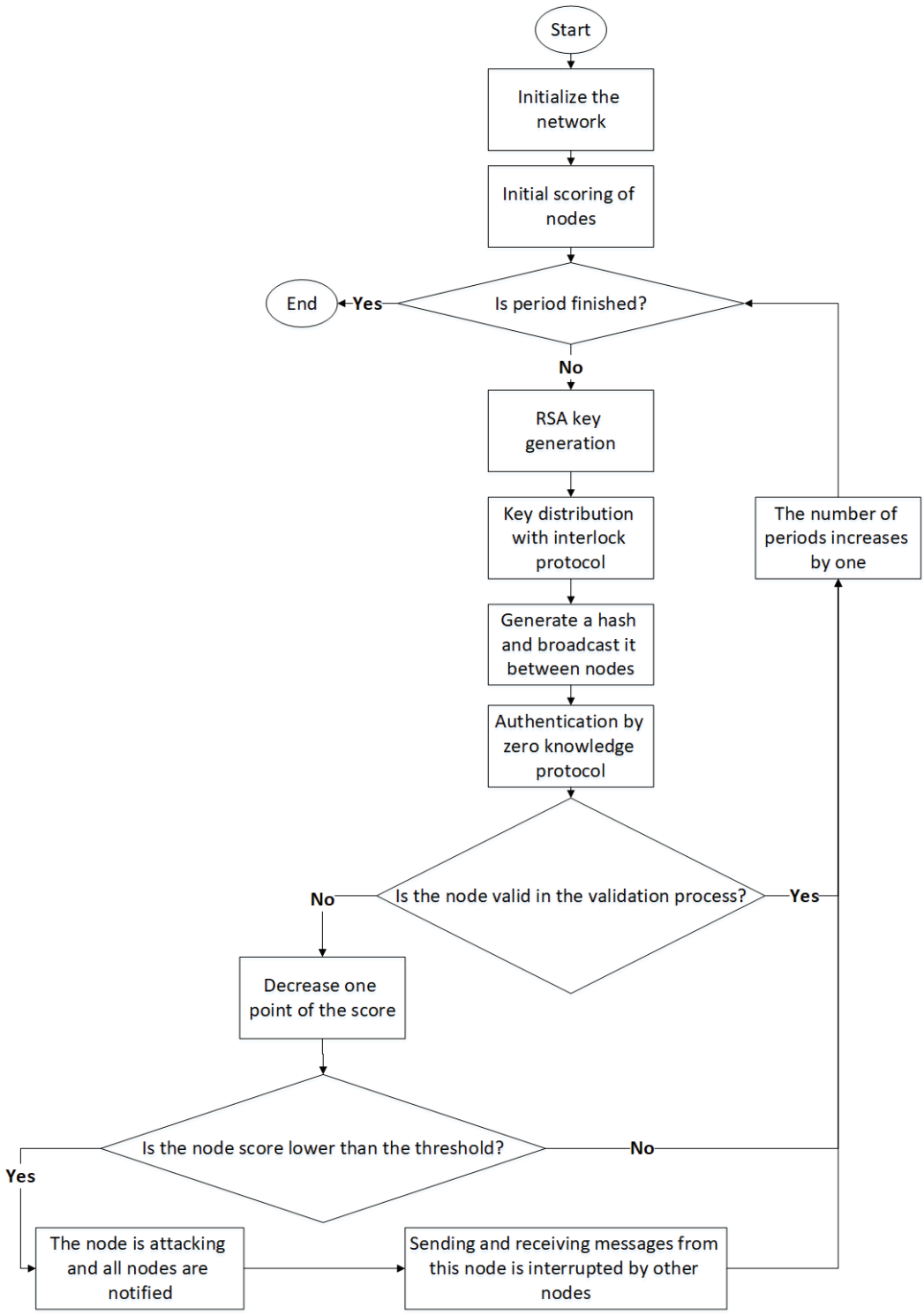

Fig. 4. Proposed workflow diagram

knowledge protocol is used for authentication, it is not possible to guess random numbers. By implementing the zero knowledge protocol, the possibility of authentication error is reduced by up to 50% each time. Here the private key S remains a mystery in the proof. Doing so makes it difficult to obtain S from Equation (3).

1. Detect an attack in the proposed method

The steps of performing this algorithm in the proposed system are as follows (in this proposed algorithm, nodes are considered as game pieces in game theory and sending messages as a movement in the game):

- The base station generates public keys using the RSA algorithm.
- These keys are distributed between nodes using the Interlock protocol.
- In this proposed method, the node that sends the sleep synchronization message acts as the proverb and the receiving node acts as the message authenticator.
- Each node has a private key, known in this method as the S key.
- Here the public key providers and certifiers share.
- The proof node generates v and hashes it by holding the public key, the private key and using relation (3). In a way, it can be said that this generated key is the same as the secret key of the corresponding node, and it can be seen that in this case, it is possible to discover the key with a very low probability.
- On the confirmation node side where this message is received, the secret key of the receiving node is requested from the base station, in which case the authentication node can perform authentication.
- If v received from the base station and v received from the proof node in the authentication node are checked and these two keys are the same, the authentication will be successful and the node score will not be reduced, otherwise the authentication will not be successful and the score of the node is reduced. If the score of the proving node falls below the threshold, it is identified as the attacking node, and therefore all messages received from the attacking node are then passed by the acknowledging node, resulting in the DoS attack failing here, and the proposed method can Detect this type of attack with very low overhead.

VI. EVALUATION

MATLAB software version R2017b 64-bit was used to simulate the program. This software makes many application functions readily available.

A computer with the hardware specifications of Table I was used to simulate the proposed algorithm.

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

In this simulation, we must first specify the number of nodes. Nodes use the SMAC protocol to update sleep time. During the simulation, the AODV protocol was used to route the nodes. The simulation time is estimated at 50 milliseconds. In this simulation, the initial energy of each node is set to 1000 mW. The channel used in this simulation is a wireless channel. The SMAC protocol is used as the MAC protocol. It consumes 0.014 mW for idle time and 0.036 mW for sending. Also, for sleeping nodes, the energy consumption is 0.000015 mW. The energy required during the transition from one state to another is 0.028 MW. In this simulation, the base station uses the RSA algorithm to generate the keys. The data parameters for the simulation are as 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

In the diagrams presented in this section, the

x-axis shows the simulation time and the y-axis shows battery energy, packet delivery rate, and output power, respectively, and the attacks that are attempted to be prevented here are DoS attacks.

Fig. 5 shows the amount of battery energy used during the simulation. It can be seen that in the event of a DoS attack, the grid energy is drastically reduced, causing premature node death. Here it can be seen that the energy of the nodes is drastically decreasing and this part is shown in red using the color. Here the attack is prevented using the zero knowledge protocol for SYNC message sending nodes. In general, the red diagram shows a state in which the destructive node has not been identified, and it can be seen how the energy is reduced in this state. The blue diagram shows that by protecting the nodes from attack, the lifespan of the sensor network is significantly improved. However, in the proposed method of this research, due to multi-stage authentication, a little more energy is consumed than usual, so it can be seen in the graph obtained that the proposed method is worse than normal and consumes more energy, but from a point of view. After the destructive node is identified in the proposed method, the energy consumption of the nodes becomes normal and ideal, while in the red diagram, a decrease in energy can still be seen. In this case, the network under consideration disappears much faster than the proposed method network. The proposed method will definitely have a longer lifespan and due to the use of game theory is able to identify malicious nodes with a much lower overhead.

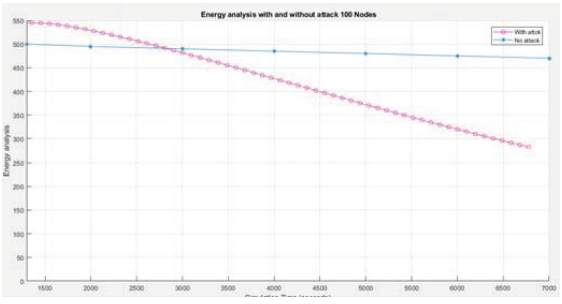

Fig. 5. The amount of battery energy used during the simulation

In the diagram in Fig. 6, by comparing the packet delivery rate with attack and without attack, we show that in case of attack prevention, the performance of the sensor network is improved. The red graph shows the attack scenario in which the packet delivery rate was initially high, but with repeated packets being played by the attacking node, a sharp drop in the packet delivery rate is observed after the node battery is discharged, as described in the previous diagram. Initially, the package delivery rate in the proposed method is low, and this is due to the operations required to authenticate and identify malicious nodes. In the proposed method, after the malicious nodes are identified and also authentication is done for all nodes, the packet length rate increases because in the proposed solution of this research, authentication is done first and after identification, each time authentication is done, so we can say that there is only one initial overhead in the proposed method.

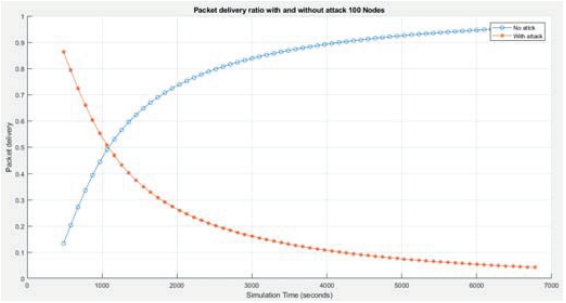

Fig. 6. Package delivery rate in attack mode and without attack

In Fig. 7, the output power is improved as the attack is prevented. In the case of preventing an attack, the output power of the sensor network is improved. The red diagram shows the attack scenario, which is reduced by the repetitive distribution of packets by the attacking node after the node battery is discharged.

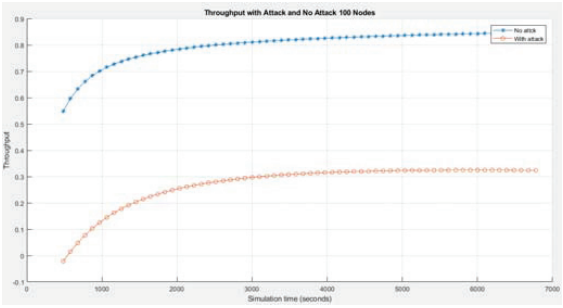

Fig. 7. Output in attack mode and without attack

Over time, the existing destructive nodes increase the waiting time, and in a way it can be said that in this case, the overhead will reduce the operational power and cause poorer network

performance, which can be shown in Fig. 8 average waiting time in a normal network. The presence of an attack was observed. Of course, this waiting time is not present in the proposed method because in this proposed research solution, malicious nodes are detected quickly, and in this case there will be no waiting time due to the presence of malicious nodes. Nodes are not exchanged to increase the waiting time in the proposed method network.

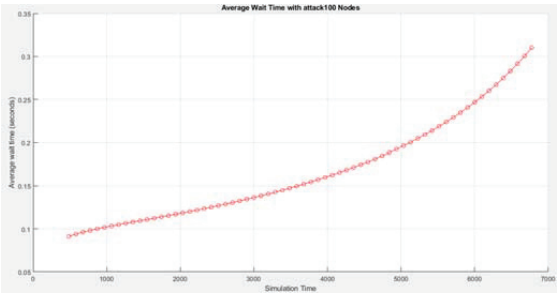

Fig.8. The average waiting time on a typical network despite an attack

In Fig. 9 we can see the error rate at the time of simulation for the proposed method and the normal case. It can be seen that in the normal case, the error rate gradually increases, but in the proposed method, this rate is zero, and this is due to the existence of a method in which no error message is sent and if the node is authenticated, the package is sent. According to the proposed protocol, the destructive node cannot be properly authenticated.

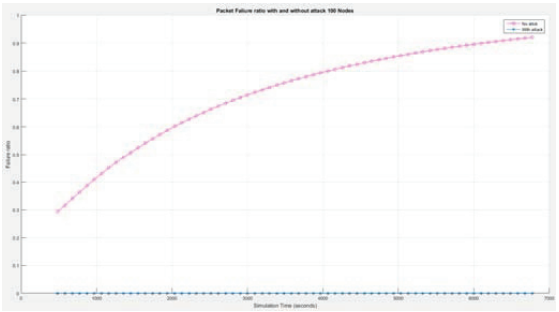

Fig. 9. Closed error rate in a typical network despite the attack and the proposed method

The results of the proposed work are being compare with the Zhang approach[21], Ranjeetha approach [22] and Tao approach [23], Turki Approach [24] as shown in Fig. 10. These are the different approaches that give security to WSNs. Fig. 10 shows the entire number of packets the receiver has sent vs the rate of Packet Loss.

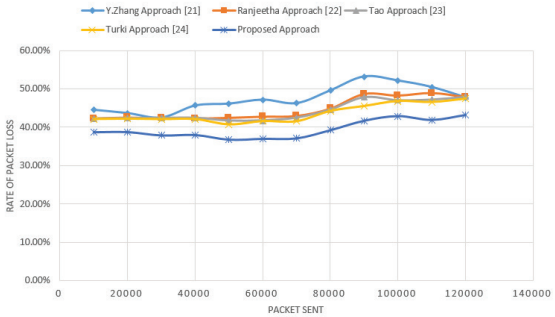

Fig. 10. Packet Sent vs Rate of Packet Loss

As can be seen, the proposed method is able to have a less Rate of Packet Loss compared to other methods, and this is a sign of higher security and also higher accuracy of the proposed method.

VII. CONCLUSION

This dissertation proposes a new scheme for the validation and authentication of malicious nodes that seek to change the sleep schedule of nodes. The proposed scheme is based on the zero knowledge protocol and game theory to validate and authenticate sensor nodes that exchange sleep synchronization messages. In the proposed method, in order to increase security, the Interlock protocol was used to exchange the key. In the proposed method, all nodes that send the SYNC message are validated before the message is accepted or rejected. Therefore, the proposed method is an effective way to prevent sleep deprivation attack. In the proposed method, the attacking node cannot redistribute the sleep synchronization signal because sleep time without authentication is not acceptable. Nodes in sensor networks have limited resources and capabilities. Most importantly, overuse of network resources may reduce network lifespan. The proposed method uses the authentication mechanism of nodes that try to send SYNC packets to prevent sleep deprivation. This is done using the zero knowledge protocol. By preventing the attack, the simulation results show that the network life is improved. Despite secure connections within the network, this defense mechanism also extends the life of the network. In other words, this dissertation presented a new security framework

that provides a comprehensive security solution to vulnerabilities. The combination of the zero knowledge protocol with the interlock protocol for key transfer made the packages protected against popular attack; therefore, the proposed method consumes less network resources and is a suitable security approach for wireless sensor networks.

One of the suggestions that can be made is to provide a solution for reliable clustering in such a way that malicious nodes can be identified in clusters and two types can be considered for each of the normal clusters: normal clusters and virtual clusters using game theory. Attribute the nodes to these two clusters, ie the nodes that have the appropriate score are in the list of real clusters from the beginning and the nodes whose score is low for various reasons are added to the list of virtual clusters and the nodes that are in the list of virtual cluster nodes. They cannot be sent and received, and as a result, security in receiving and sending packages can be increased.

REFERENCES

1. K. Sharma and S. Pradhan, "Cluster Head Rotation in Wireless Sensor Network: A Simplified Approach," International Journal of Sensor and Its Applications for Control Systems, vol. 4, no. 1, pp. 1-10, 2016.

2. S.-H. Seo, J. Won and S. Sultana, "Effective Key Management in Dynamic Wireless Sensor Networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2015.

3. A. Abbasi and Y. M, "A survey on clustering Algorithms for Wireless Sensor Networks," Computer Communications, vol. 30, pp. 2826-2841, 2007.

4. "Energy efficient homogenous clustering algorithm for wireless," Internations journals of Wireless Sensor Network, vol. 2, pp. 49-61, 2010.

5. F. Akyildiz and M. lan, Wireless Sensor Network, Wiley, 2010.

6. A. Laszka, M. Felegyhazi, L. Buttyan, "A Survey of Interdependent Information Security Games," ACM Computing Surveys, vol. 47, no. 2, 2015.

7. W. Saad, T. Alpcan, T. Basar and A. Hjorungnes, "Coalitional Game Theory for Security Risk Management," Fifth International Conference on Internet Monitoring and Protection, pp. 35-40, 2010.

8. J. Grossklags, N. Christin and J. Chuang, "Secure or insure?: a game-theoretic analysis of information security games," Proceedings of the 17th international conference on World Wide Web, pp. 209-218, 2008.

9. Y. E. Sagduyu, R. A. Berry and A. Ephremides, "Jamming games in wireless networks with incomplete information," IEEE Communications Magazine, vol. 49, no. 8, pp. 112-118, 2011.

10. M. Fallah, "A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory," IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 1, pp. 5-19, 2010.

11. L. Chen and J. Leneutre, "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks," IEEE Transactions on Information Forensics and Security, vol. 4, no. 2, pp. 165-178, 2009.

12. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, J.-P. Hubaux, "Game theory meets network security and privacy," ACM Computing Surveys, vol. 45, no. 3, 2013.

13. Z. Zhou and Z. Sun, "A Lightweight and Dependable Trust Model for Clustered Wireless Sensor Networks," Cloud Computing and Security, vol. 9483, pp. 157-168, 2015.

14. G. Dogan and K. Avincan, "MultiProTru: A kalman filtering based trust architecture for two-hop wireless sensor networks," Peer-to-Peer Networking and Applications, pp. 1-14, 2016.

15. D. Fang, L. Gao, Z. Tang and X. Chen, "A Software Protection Framework Based on thin virtual machine using distorted encryption," 2011.

16. P. Bommannavar, T. Alpcan and N. Bambos, "Security Risk Management via Dynamic Games with Learning," IEEE International Conference on Communications, pp. 1-6, 2011.

17. S. Mirjalili, L. A. Mirjalili, "The whale optimization algorithm," Advances in Engineering Software, vol. 95, pp. 51-67, 2016.

18. D. R. R. a. S. F. M. Bradley, "Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks," IEEE, 2017.

19. V. Tiri, M. Night, T. axis, S. Parbat, "Zero knowledge protocol to design security model for threats in WSN," Int. J. Eng. Res. Appl.(IJERA), vol. 2, pp. 1533-1537, 2012.

20. R. Sangeetha, Y. M. Sangeetha, "Secure energy-aware multipath routing protocol with transmission range adjustment for wireless sensor networks," In Computational Intelligence & Computing Research (ICCIC), pp. 1-4, 2018.

21. Y. ZHANG, C. WU, J. CAO, X. LI: A secret sharing-based key management in hierarchical wireless sensor network, International Journal of Distributed Sensor Networks, 9(6), 406061, 2013.

22. S. RANJEETHA, N. RENUGA, R. SHARMILA: Secure zone routing protocol for MANET, International Conference on Emerging Trends in Engineering, Science and Sustainable Technology, (ICETSST), 67-76, 2017.

23. T. YANG, X. XIANGYANG, L. PENG, L. TONGHUI: A secure routing of wireless sensor networks based on trust evaluation model, Procedia Computer Science, 131 (2018), 1156- 1163.

24. A. T. ALGHAMDI: Convolutional technique for enhancing security in wireless sensor networks against malicious nodes, Human-centric Computing and Information Sciences, 9(1), ID38, https://doi.org/10.1186/s13673-019-0198-1, 2019.