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 3, 2023. ISSN: 2348-6600
Reference ID: IJCS-466 PAGE NO: 3175-3182

WSNS SECURITY ENHANCEMENT BASED ON A GAME THEORY

M. Malini
Research Scholar,
Department of Computer Science,
Marudupandiyar College of Arts and Science,
(Affiliated to Bharathidasan University),
Thanjavur, Tamil Nadu, India.

Dr. U.Durai
Research Advisor,
Department of Computer Science,
Marudupandiyar College of Arts and Science,
(Affiliated to Bharathidasan University),
Thanjavur, Tamil Nadu, India.

Abstract:

This script investigates how game theory might enhance community security in wireless sensor networks. Large numbers of sensor nodes that are deployed randomly or in a predictable pattern make up wireless sensor networks. The goal of this project is to provide wireless sensor networks with network protection so that detection information may be efficiently transmitted to the receiver, extending the system's lifespan. To perform this task, an unique protocol was developed using game theory. The mathematical analysis of interactive decision-making processes is supported by game theory. It provides resources for forecasting what could (and ought to) happen when actors with competing interests interact. It is not a singular approach, but rather a collection of modelling tools that aid in the grasp of interactive decision-making to solve problems. The proposed Game Theory methods are successfully applied to prevent Denial of Service attacks, to identify and guard against malicious sensor node behaviour in Wireless Sensor Networks, and it has been demonstrated that the operation of those games significantly reduces tunnel misbehaviour, conserves node power, and extends the network lifetime economically. Using Network Simulator NS2, the suggested approach was tested and confirmed through simulation.

Introduction

The first section of the article uses the auction notion, which makes it possible to find cooperative nodes, to highlight the need for safety enforcement. Nodes in the protocol desire to participate in forwarding incoming bundles and improve their reputation. Nodes that are motivated to accomplish this should compete with one another. The contest is based on the idea of an auction. In this stage, we recommend a reliable, protected auctioning-based routing system for sensor networks. Auctions can provide efficient allocations with the right design principles and little a priori knowledge. The primary reason to use the first-price sealed auction system at the process established in this phase is to speed up the purchase and encourage competition between bidders, which is one of the important reasons to use auction. Since sensor networks lack pre-existing infrastructure, the bulk of the nodes might serve as traffic routers. Both good and bad sensor nodes fight with one another to transmit incoming packets since doing so improves each node's position relative to the other nodes. Instead of paying cash, bids are made in order to improve one's position in the community; the winner of the bid forfeits some of the community's first energy power.

The decision to participate in a market is totally up to the detector node, as opposed to a malicious node that makes every effort to win the bid, then throws in the towel and corrupts the community.

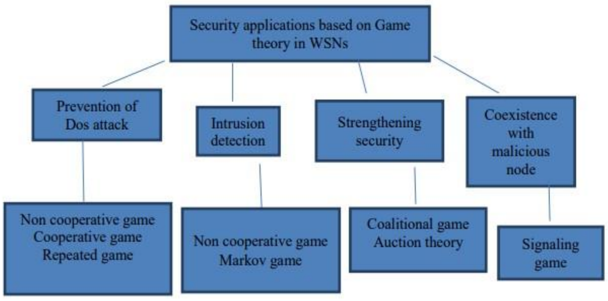
Related work

But before WSNs are widely used, WSNs safety is a crucial and vital issue. This necessitates the necessity for diverse countermeasures for WSN strikes. A qualitative decision frame for WSN safety is required during training. Game theory simulates scenarios in which numerous players compete with one another for resources; it can provide a mathematical framework for simulating and examining WSN safety problems. So it seems sense to use game theory to address the security issues with WSNs. The existing approaches to wsn safety are reviewed in this section. All pertinent articles are divided into two groups: non-cooperative game idea and cooperative game theory. The current common game theoretic tactics are designed to strengthen WSN security. These techniques are divided into four categories based on specific secure software: avoiding DoS assaults, intrusion detection, enhancing security, coexisting with hostile detector nodes using cooperative games, and noncooperative games. The articles contain a good deal of the most recent research on game theory methods for WSN intrusion detection. In order to address potential improvements and potential problems in nodes and base stations, Kuldeep et al. recommended a smart safety representative (ISA) at WSN. Although ISA in node level with cross-layer technique may provide significantly better safety, node level execution will be extremely difficult. Confidentiality, information integrity, service accessibility, and vitality were some of the potential solutions Krishnan discussed in relation to the four aspects of WSN safety. In addition, Krishnan described the match version for power savings in order to obtain suitably big source restricted networks after sharing the cluster-based safety. Alpcanetal discussed a two-player, zero-sum Markov safety game with witches and IDS and looked at different game settings using numerical examples. There aren't many occasions when players' strategies were altered in response to information discovered through game theory research in order to increase the likelihood of finding this invader using sampling method. The algorithms proposed by Kodalam et al to sample networks have been evaluated. assuming that each node is aware of its maximum forwarding rate and maintains a record of interactions on the speed at which its dispatch requests are honoured. However, a node will reject a forwarding petition if it is beyond of its healthy working bounds (highest speed) or if it is intentionally routing more packets than the other nodes in the cluster. This later condition permits a modest number of surplus forwardings, which comprise the algorithm's most forgiving component.

Security applications based on game theory in WSN

A changing network topology is a result of the WSN's awful nature, which includes node scans that enter or exit the system. As a result, there is no set route for data replication. In addition to the ambiguity of these nodes, a serious issue might arise if a malicious attacker enters the system. Additionally, a power constraint may cause a node to behave egotistically in order to save energy, which increases the risk of a network outage. Therefore, the aforementioned characteristics of WSNs make their security protocols more difficult to implement and insecure. As a result, interest in WSN safety has increased. To address specific security threats posed by WSNs, certain techniques were developed. In WSNs, a variety of security techniques are used, all of which call for the standing principle. All of these reputation-based techniques fall within the scope of this overview article because the main focus of this work is on game-theoretic security techniques. It deals with problems where pricing functions of distinct entities are interdependent. The authors discuss the positive aspects of game theory for wireless networks, while various trends in employing game theory for WSNs are examined. The game notion has recently made its way into decentralised communication techniques with the creation of infrastructure-less and distributed systems. One of the difficulties in this class is related to WSN safety. The interaction between guardian(s) and participant(s), which is required for the safety issue, may be directly translated into a player match in which each player tries to promote their own advantage.

The reliability mechanics are thought to be the main worry of these WSN safety experts. Figure 1 depicts the general workflow of a confidence model, similar to the version taken into consideration. There are four main steps to this trust model. The first stage is gathering data from the traffic flow, and the second stage involves putting the accepted trust model into practise. In the following phase, the intrusion detection algorithm evaluates the inspected data from the confidence model. The fourth stage is in charge of either punishing or rewarding the corrupted or helpful pliers. This mechanism's overarching goal is to develop robust, efficient systems.


Security applications based on Game theory in WSNs
Prevention of Dos attack
Intrusion detection
Strengthening security
Coexistence with malicious node
Non cooperative game Cooperative game Repeated game
Non cooperative game Markov game
Coalitional game Auction theory
Signaling game

Applying the general concept of learning automata by sampling the incoming programmes, one may defend against the intrusion effect. Using game theory, the same technique may be applied to increase the security of WSNs. The personality of WSN needs to be taken into account while building the sport version. Maintaining precise data transfer from many nodes, preserving low energy consumption, accommodating a large number of nodes, and providing prompt conclusion are all essential to the WSN's operation. In actuality, the different game theoretic strategies rely on standing to establish strong trust models in opposition to the WSN risk circumstances. The version first targets the greedy nodes. The model in the following situation covers the lymph nodes that your WSN deems injured. In the end, the WSN is adversely affected by greedy and malevolent nodes, which is why a smart version is desired. We examine several game security measures against various attack vectors in WSNs in the discussion that follows. Depending on the sort of attack and the expected penalty, a combined or noncooperative sport may be chosen.

Proposed Work

In this chapter, we provide two different methods for assessing the use of the game-theoretic framework. For unblocking hostile nodes and providing protected routing in wireless sensor systems, a protected sensor system routing protocol based on an auction idea frame is proposed. Nodes like to participate in forwarding incoming bundles and build a name for themselves in the neighborhood. Nodes that are motivated to accomplish this should compete with one another. The contest is based on the idea of an auction. Each node offers a bid sum equal to its utility value, and the price the winner of the bidding must pay is a reduction in its starting power. Even malevolent nodes that do not bid honestly must be distributed in order to have a secure routing protocol since honest node bidding continues to be the majority strategy. Secure Auction based Routing (SAR), our recommended method for avoiding specific types of strikes, includes each course's whole bid as data packets.

Describe the protocol

Unless they have already received the exact same request, all nodes receiving this information put themselves in the source path and forward it with their own neighbours. When a receiving node has a path to the destination or is the destination itself, it does not transmit the request but instead sends a reply message instead that includes the full source path and the bid price it is willing to accept. The source receives a few pathways, picks the one with the highest bid, and saves it to transmit messages over the route. The route is chosen from the SAR process by selecting the largest bid route from the cache of all accessible routes to the package's destination, as shown in Figure 2. The route this path petition has gained is cancelled and sent back to the sender after a course request has arrived at its destination. This protocol proposes a route auction to ensure perspective on which nodes may potentially provide service due to their devotion. Be mindful that a rogue node might participate in the auction and pervert the route; a watch-list makes it easier to spot such problematic ecosystems. When the auction is over, the transmitting node transmits a winning route package to the destination node, which saves this path along with the origin, enabling the receiving node to be able to perform the timeout. The origin is removed from the list of pending links when the destination node gets a packet from the origin that isn't a control packet. The destination node sends a Bad route packet into the bottom channel if the waiting connection times out, which updates its record with all the nodes from the path (excluding the destination and source). The base station sends out a Watch list dismiss air, and each node adds the node to their ignore lists when it is added to the watch list more frequently than a certain threshold. The threshold is high enough to distinguish a node's effortless selfishness from intentional malevolent behaviour. Every node would rather not communicate with a node on their ignore list.

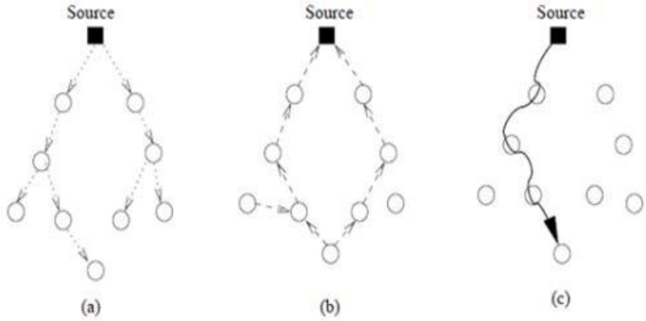


Figure 2: (A) Route request (B) Route reply (C) Establishing the path

Players make decisions in strategic games first, after which the game's conclusion is decided. Either determinism or uncertainty may be present in the result.

The choices are made independently of those made by other players. There are N players who compete to bid against one another in a sensor network made up of N sensors, some of which sometimes engage in malevolent behaviour.

A finite collection of N sensor nodes make up the strategic game known as "bidding," and for each node I = 1 through N, there is a nonempty set Ai of actions that are accessible to it. For each node I there is also a von Neumann-Morgenstern utility function ui R:Ai, where R is the set of real numbers.

No extra node would wish to stray at this point. Every node may only genuinely bid for a maximum amount of its own utility. We are aware of the balance's location (which depends on the payoff value now calculated), and the system will demand the appropriate bid acceptance based on the payoffs calculated. To put it another way, the balance tells us which bidder from the sport makes the most sense in a given situation, and the system does as it is told. The possibility of sensor node connection and computation has been considered in order to determine the necessary power for each sensor node. Compared to computing, communication consumes a lot more energy. The system's connectedness, which is defined as the ability to link any two nodes, determines how well a sensor network can communicate. The number of hops, latency, etc., affect the cost of connectivity. We now calculate the connectivity energy consumption in a course with three nodes as a function of energy at each node and the total number of enroute hops. A participant or node is aware of its own appraisal of the package but is unaware of other bidders' evaluations. Nash equilibrium is a tactical match's alternate. Every tactical game with a given number of players who can each only do a certain set of actions has stability. At this Nash equilibrium, no participant wants to unilaterally depart from the situation. Each of these N > 1 potential bidders is aware of the maximum price it will accept (vi). The decision issue for each node may be viewed as choosing a bidding strategy and winning odds (b(vi)). If b* is the equilibrium bid strategy, someone may demonstrate that it is monotonically growing in v, ensuring that the highest-testing bidder will win the auction.

Simulation

We incorporate a timer to simulate spoofing. The timer will be started at the beginning of the simulation. A "spoof" component is activated at the node when the timer expires, and the timer is then automatically reset. Once the "spoof" component is in place, all that the node needs to know is the origin address of another incoming route request. The simulation of this suggested technique is run on the NS2 period, which was chosen to be long enough to potentially float, and the total numbers of lost packets are only about 1.

Table 1: Simulation parameters

parameters	values
Area	1000m x 1000 m
Speed	Uniformly 0-20m/s
Radio Range	250 m
MAC	802.11
Sending capacity	2 Mbps
Simulation time	1000s
Auctions last	60s
Timeout at receiving node	20s

All of the location. Sensors use the Random Method stage model, in which detectors move at a uniformly distributed pace to a random location. A standard DSR system is used as the initial network under test and serves as a baseline. Numbers 1 and 2 show that the average number of packets lost changed across the pause days but that the proportion of malicious nodes remained the same. There are three different types of attacks that can be made against a sensor system: (I) IP spoofing attack, in which a malicious node pretends to be someone else, (ii) the black hole attack, in which a malicious node from the trail violently discards messages that are routed through it, and (iii) feign trail error message assault, which is repaired in a third of their total number of nodes, such as 10 and 50 nodes, respectively. Furthermore, in the instance of 50 nodes, we observe that at SAR, the average number of lost packets remains consistent but there are 2/3 less CONFIDANTS. This is because at SAR, nodes with a bad reputation will likely be dismissed by the majority. Wherein a malicious node sends a regular node trail error messages to indicate a broken connection and therefore diverts the path. We have calculated the average number of packets lost in relation to the total number of malicious nodes in the community. The navigational overhead has also been computed. Table 1 contains the altered parameters, including simulation experiments.

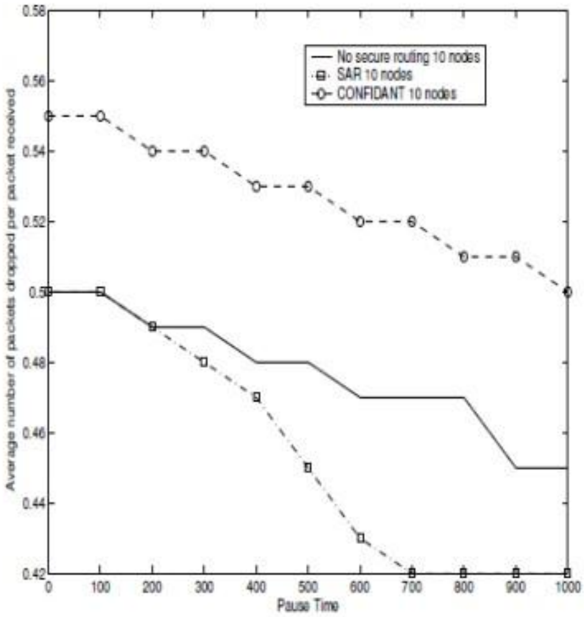


Figure 3: Mean number of packets dropped versus pause time, one third of malicious, 10 nodes

According to Fig. 3, when more lymph nodes are added overall, more packets will experience a drop due to the lymph nodes' negative roles. But with time, the total number of missed packets will decrease in SAR. The fundamental reason is because, in a system with nodes, nodes may eliminate bad reputational nodes, but in a smaller community, nodes cannot be eliminated equally, and periodically, only some nodes must be chosen to relay incoming messages.

Conclusion and future work

We created the SAR protocol and examined its operation. Our aim was to evaluate how effective various techniques were in spotting malevolent behaviour. The testing findings show that we might provide more dependable shipping by using an auction created frame and combining the utility value of every route that is based on energy power and lymph node standing. We might also watch sensor node behaviour and separate shady ones by setting an appropriate threshold for the usefulness of sensor nodes. One further goal we have in mind is to observe how our proposed routine performs when a group of bidders band together and agree not to duplicate one another, which has the overall impact of lowering the winning price. Exemptions are granted for quite varied reasons. In essence, the bidders consent to lessen competition by avoiding direct competition. We're interested in seeing how this could impact the way nodes cooperate. A separate, occasion-specific simulator for modelling wired and wired community circumstances is known as Network Simulator 2, or NS2. MICA2 sensor nodes would be used in this situation. On Mica2, we have put our suggested safety authorities' tactics into practise. In addition to a flexible detector board with many detection modalities, we have employed string detectors. In order to build sensor networks for a variety of applications, including sensing, motion, etc., these modalities may be used. A very basic photocell known as a light detector is part of the MTS510CA. The electrical command signal PW0 must be turned on in order to use the light detector.

References

1. Game Theory and Wireless Sensor Networks: An Overview, by Bijaya Ketan Panigrahi, Charanjit S. Jutla, in Wireless Sensor Networks: Recent Advances and Future Challenges, by Charanjit S. Jutla, Bijaya Ketan Panigrahi, CRC Press, 2016.
2. Game Theory in Wireless Sensor Networks: Overview and Challenges, by Zhenhai Zhu, in Wireless Sensor Networks: Selected Research Topics, by Zhenhai Zhu, Elsevier, 2016.
3. Game Theory for Wireless Sensor Networks: A Tutorial, by H.V. Poor, in Wireless Sensor Networks: From Theory to Applications, by H.V. Poor, Cambridge University Press, 2011.
4. Game Theory for Wireless Sensor Networks: A Survey, by S.K. Das, S.K. Das, in Wireless Sensor Networks: Architectures and Protocols, by S.K. Das, Springer, 2008.
5. Game Theory and Wireless Sensor Networks, by X. Li, W. Lou, in Wireless Sensor Networks: Technology, Protocols, and Applications, by X. Li, W. Lou, Wiley, 2008.
6. Game Theory in Wireless and Sensor Networks: Fundamentals and Applications, by Kamal Jain and Vinod Sharma, 2018.
7. Game Theory for Wireless Networks: Theory, Models and Applications, by Geert Heijenk and Joost Kok, 2016.
8. Game Theoretic Methods in Wireless Sensor Networks: From Theory to Reality, by Wei Yu et al., 2012.
9. Game Theory in Network Security: A Comprehensive Introduction, by Günter Schäfer, 2016.
10. Game Theory and Signal Processing for Wireless Communications, by Wei Cai and Shuguang Cui, 2013.

11. Game Theory for Networks: An Introduction, by Mihaela van der Schaar, 2012.
12. Game Theory in Communications: Theory, Applications, and Networks, by Jun Wang et al., 2016.
13. Game Theory in Wireless and Communication Networks: Theory, Models and Applications, by Tamer Başar and Geert Heijenk, 2010.
14. Advanced Topics in Wireless Communications and Networks: Game Theory and Network Security, by Lajos Hanzo et al., 2011.