Detection of False Node in WSN using Non Cooperative Non-Zero Sum Game Theory

P. Hema[#1], V. Vinoba[*2]

1. *Department of Mathematics, R.M.K College of Engineering and Technology, Research Scholar in Bharathidasan University, India.*

2. Department of Mathematics, K.N. Govt. Arts College for Women, Thanjavur, India

Abstract *Wireless Sensor Network (WSN) is an auspicious technology that has tremendous potential for various futuristic applications. As WSN become wide spread, security becomes a cardinal affair.* Wireless sensor networks has grown a lot in recent years and offers excellent opportunities in defense related applications such as monitoring environment and collecting data related to antisocial activities. Currently, the needs of wireless sensors have become inevitable in daily life. With the continuous growth of Wireless sensor networks in daily life, business, and defense applications, the security of transferring data from sensors to their destination has become an important research area. Due to the limitations of power, storage, and processing capabilities, current security mechanisms of wireless networks or wired networks can not apply directly to wireless sensor networks. So there is a need to develop new techniques or modify the current security mechanisms to transfer data from source (from the field) to base station (destination). In this paper, we discuss currently available intrusion detection techniques, attack models using game theory, and then propose a new framework to detect malicious nodes using zero sum game approach for nodes in the forward data path. The first part of research provides the game model with probability of energy required for transferring the data packets. The second part derives the model to detect the malicious nodes using probability of acknowledgement at source.

Wireless sensor networks, game theory, zero sum non zero sum non cooperative game theory processing capability, security, deployment, Nash equilibrium.

I. INTRODUCTION

The unique characteristics of sensor networks limit the applicability of traditional security measures. Since sensor nodes have limited power sources, limited local memory and calculation capacity, they are not able to store long-sized keys or run complex cryptology algorithms. Usually sensor nodes are densely deployed, and may not have a global identification number because of the large amount of overhead. They may also fail due to lack of power or physical damage. The dynamic nature of sensor networks' topology is typically due to node failure or node insertion instead of node mobility since most sensor networks applications do not assume a highly mobile characteristic. Most of the applications of these WSNs are unattended. The WSNs deployment area may not be possible to approach, since the environment may be hostile and dangerous. Therefore, WSNs must be autonomous and exhibit responsiveness and adaptability for evolution changes in real time. Due to these reasons, the network operation requires appropriate administration to acquire the data. The autonomous nature of WSN nodes and their limited resources makes them susceptible to attacks. To provide normal operation of these WSN nodes, we must provide some mechanism within the network itself. The conventional security techniques cannot be used directly in WSNs because of following unique characteristics:

1. The low cost and resource restrained in terms of energy, memory, computation, and communication Capabilities
2. They may be deployed in public hostile
 locations, where they are vulnerable to physical attacks by adversaries
3 The hackers may take control of sensor nodes and extract secret information
4. Due to basic properties of the nodes, they may be dynamically reorganized and use insecure communication

As a result, existing security mechanisms are inadequate, and new approaches are desired. WSNs are vulnerable to many attacks because of broadcast nature of transmission medium, resource limitation on sensor nodes, and uncontrolled environments where they are left unattended. Similar to other communication systems, WSNs have the following general security goals:

2. SECURITY GOALS

When dealing with security, one is faced with achieving some or all of the following goals

• **Availability**: Network assets are available to authorized parties when needed and the sensor network should ensure the survivability of network services despite denial of a service (DoS) attack. To ensure the availability of message protection, the sensor network should also protect its resources to minimize energy consumption .

- **Authenticity:** An adversary might easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from a trusted source.
- **Confidentiality**: A confidential message is resistant to revealing its meaning to an eavesdropper. Confidentiality should be provided by keys with as small a scope as possible, to discourage a single break from compromising a large portion of the network.
- **Freshness**: It implies that the data is recent and ensures no adversary replayed old messages.
- **Data Integrity**: It ensures that the received data is not altered in transit by an adversary.
- **Scalability**: Sensor networks cannot utilize a keying scheme that has poor scaling properties in terms of energy cost or latency. In general, the number of neighbours and the distance or power required to send messages from one node to another will not be known in advance.

3. Game Theory: A Brief Overview

Game theory is an advanced branch of intelligent optimization. The model of game theory represents a game between player groups that choose to behave cooperatively or non-cooperatively and try to promote their benefits (payoffs) through the used strategy(ies) executed through the cumulative players actions. survey the fundamental definitions of game parameters, which can be summarized as follows:

Definition 1. A game is a description of the strategic interaction between opposing, or cooperating, interests where the constraints and payoff for actions are taken into consideration.
Definition 2. A player is a basic entity in a game, which is involved in the game with a finite set of players denoted by N that is responsible for taking rational actions denoted by A_i, for each player *i*. A player can represent a person, machine, or group of people within a game.
Definition 3. The Utility/Payoff is the positive or negative reward to a player for a given action within the game denoted by $u_i : A \rightarrow R$, which measures the outcome for player i determined by the actions of all players A = $X_{i\in N} A_i$ where the symbol X denotes Cartesian product.
Definition 4. A strategy is a plan of action within the game that a given player can adopt during game play denoted by a strategic game . $\langle N, \langle A \rangle, \langle u_i \rangle \rangle$
In the security field, game theory application is not only limited to counteracting the effect of external intruders; it can be used to detect the malicious nodes and reveal the nodes that behave selfishly and overburden the whole network. Generally, Nash equilibrium (NE) is the intelligent solution for the social problems that has become a promising concept for wireless networks and more specifically for WSN security

Definition 5. Nash equilibrium is a profile of optimal actions $a^* \in A$ such that any player $i \in N$ cannot benefit due to unilaterally deviating from its strategy and choosing another action. This can be translated in terms of the utility function as, $u_i(a_i^*, a_{-i}^*) \geq u_i(a_i, a_{-i}^*)$ for all a_i denotes the strategy of player *i* and a_{-i} denotes the strategies of all players other than *i*. Nash equilibrium is the intersection of best responses. In NE each player is playing his best response to the actions of all the other players.

3.1 Zero-Sum Game

The zero-sum game is one of the types of non-cooperative games between two players. One player is considered a maximizer that strives to maximize its gain while the other is considered to be the minimizer that aims to minimize its losses. Consequently, it seems as a two-side conflict game or a one-side win game, at which the total utility/payoff of both players remains constant during the course of the game, $\sum_{i=1}^{2} u_i(s) = 0 \, \forall s \in S$ where **s** is a strategy profile . Apparently, **constant-sum game** could be transformed to an equivalent zero-sum game; and zero-sum game is a special case of constant-sum game given that the players add up their gains or losses to a constant value for any strategy profile..

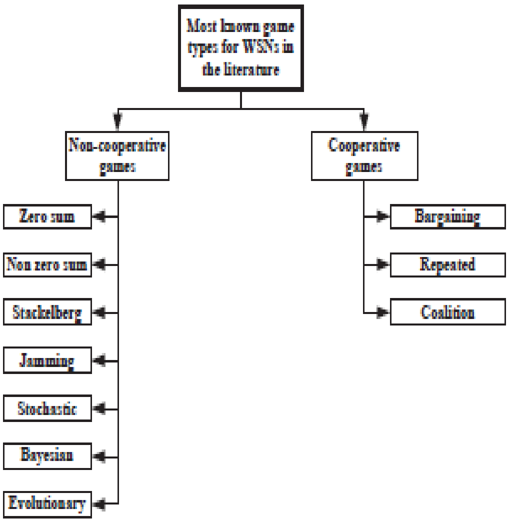
3.2 Nonzero-Sum Game

Nonzero-sum game is played between two or more players where the sum of players' utilities is not constant during the course of the game .. In nonzero-sum games, all players are considered maximizers or minimizers which have no constraints on the total utility as in the zero-sum game. Consequently, all the participants can gain or lose together.

4. Games Theory for WSNs Security

The different game types that are commonly used to model WSNs security issues can be classified to cooperative games and non-cooperative games as shown in Figure 1. The cooperative games are represented by cooperating nodes aiming at maximizing the whole networks security against different security threats. On the contrary, the non-cooperative games involve the conflicting individual actions for which every node aims at maximizing its own payoff that opposes the others' outcomes. Figure 1 lists the different types of games that have been used to model security problems in WSNs

(Figure 1 does not present a classification for games in general, but presents the games that have been used in the literature to model WSNs security problems



4.1 Attack model

In sensor networks, the main function is to transfer the data to the base station. The hackers always try to take the control of routing layer of the node so that the data flow will be disrupted. If the nodes are formed into clusters, then the cluster heads are responsible for providing the needed security for transferring the data. In such cases, the adversaries would target the routing layer at cluster head to jam the data flow or drop the packets. In order to verify the appropriate packet flow, we can use the watchdog approach to detect the malicious node. The watchdog technique was simulated by ***Ioannis et al. [2]*** and presented the effectiveness of the attack (to detect whether attach is launched or not) on the node.

In the proposed attack model, a non cooperative game theory approach for handling security issues in WSNs is proposed. The game is defined between the intruder (player 1) and the IDS (player 2) where each one tries to maximize its own payoff. For example, if we consider the cooperation of neighboring nodes, the reputation of node for packet transfer and the appropriate security by IDS, the following payoff function to transfer a packet from node i to node j at any time t is given by [10]

$$U_{i,j}(t)= \alpha\times\Omega_{i,j}(t)+\beta\times\Phi_{i,j}(t)+\gamma\times\Psi_{i,j}(t) \quad \text{--- (1)}$$

where

$\Omega_{i,j}(t)$=Cooperation; $\Phi_{i,j}(t)$ =Reputation

$\Psi_{i,j}(t)$=security level and $\alpha + \beta + \gamma = 1$

The IDS at node level maintains a table that stores the history of the packet drop rate, the selection of alternate routes, and enforcement of security levels. The IDS calculates the payoff at node level before packet transfer takes place from source (node) to destination (base station). If the payoff function bends towards the attack his means that the node is compromised (the packet may be dropped). The cluster head or sink that monitors the similar situation at all nodes identifies all such compromised nodes and isolate them from the network. If most of the nodes are compromised, a situation may arise such that they will have the ability to replace the cluster head, which is a dangerous situation. When a node is removed from the cluster, the transmission to/from that node will be ignored. Removing the node from the network (cluster head) requires regenerating the key and informing all of nodes. The normal procedure is to generate a one-way function. It generates sequence of keys to be used in message authentication code and keys are used in reverse order. This procedure helps to avoid the prediction of the future keys. To generate the nth key K_n, we use the following formula $K_n = F(k\Theta K_{n+1})$,When a node is removed, the cluster head will generate a new k and inform to the remaining nodes. In the current research, we formulate the attack-defense game as a two-player, nonzero-sum, non-cooperative game, and show that this game achieves Nash equilibrium, thus leading to a defense strategy for the network, and significantly increasing the chance of detecting intrusions.

wireless sensor network where data transfer is from the sensor nodes (N) to the cluster head with action A_i and outcome u_i. In this game model, we consider IDS at cluster head and monitor the data transfer from sensor nodes to cluster head. The attacker may attack any node in the cluster (including cluster head) and the IDS at the cluster head to defend the nodes. The IDS at the cluster head tries to maintain the normal functionality of the network by preventing the attacks while the attacker tries to disturb the network. This functionality will continue at all cluster heads as well as at the base station.

Let P_i be the probability to defend the the i node in the cluster. The probability of defending all N nodes including the cluster node is $\sum_{i=1}^{N} P_i$ .Therefore

$E_c= \sum_{i=1}^{N} P_i$ -----------(2)

Assuming the total energy is 1, the energy remained with IDS after defending the cluster is:

$E_r= 1-\sum_{i=1}^{N} P_i$ ----------------(3) where $\sum_{i=1}^{N} P_i \leq 1$. The energy needed to spend by the attacker (E_a) to compromise on the nodes must be more than the energy spend by the IDS system. Therefore

$E_a= k\sum_{i=1}^{N} P_i$ -----(4) where κ is a constant for attacker and ≥0. The node compromises depending upon the κ value as given below:

- **κ>1to succeed the attack ($E_a > E_c$)**
- **κ = 1 the attacker force is equal to IDS protection (the node may or may not compromise)**
- **κ = 0 then there is no attack on any node**
- **κ <=1 The node does not compromise**

The payoff (U) is the IDS utility cost (E_c) minus
(–) the cost to defend (E_a).
If there is no attack on the cluster, then the energy spend by the attacker must be 0 (Ea=0). Therefore we get the utility cost as
U = E_c-E_a--- (5) If the attack and protection is of the same level at all
clusters, the proposed zero sum game model will use the selective nodes in the forward data path to detect the malicious node or the payoff is the same, but this is not the case all the time. Substituting equations (2) and (4) in equation (5) we get U= 1- κ$\sum_{i=1}^{N} P_i$ --- (6)
The equation (6) shows that the attack is successful if κ>1.
If you play a single game of chess with someone, one person will lose and one person will win. In our game model, the IDS defends a node and acts as player one and the attacker as player two. In a two player game, if one player wins means the second player loses, equalling to sum of zero. The win (+1) added to the loss (-1) equals zero. Such a game is called zero sum game. Games where there can be multiple winners are called non-zero sum and they are less acceptable in sensor networks security. A zero sum game can be played with two or more players. When the game is over, there are winners and losers, and the total points awarded to the winners exactly matches the total points the lost by losers exactly. In a game, if a player loses, the experience helps to win the next game, which is not discussed in this paper.
Definition 1: An outcome of a game is Pareto optimal if there is no other outcome that makes every player at least as well off and at least one player strictly better off.

Theorem 1: A zero sum game is not a Pareto optimal.
Proof: If a change from one allocation to another can make at least one individual better off without making any other individual worse off, then it is called a Pareto improvement. An allocation is Pareto efficient or Pareto optimal when no further Pareto improvements can be made. This is often called a strong Pareto optimum (SPO). This explanation leads that our zero sum game is not Pareto optimal.

Definition 2: If the zero sum game is Pareto optimal then it is called a conflict game.
In a conflict game, none of the players benefit. The game leads nowhere. Therefore, it is suggested to design an IDs to play a conflict game, so that the intruder never wins and no node compromises. If no node compromises, then the sensor network communicates the data without any distraction or diversion.

Definition 3: We say that the game is a zero sum game if for all outcomes of a, $\sum_{i=1}^{N} U_i(a) = 0$

In particular, for a two-player game $u_1(a)= - u_2(a)$ for all outcomes of a.

Definition 4: In a zero sum game the cost of attack on a node is equal to the cost to defend a node.
This leads, the profit of an attack to the intruder equals the loss to the sensor network (loss may a cluster)

Theorem 2: A zero sum game has no pure Nash Equilibrium.
Proof: In pure strategy NE, when each player's output maximizes its profits given the output of other player. For example, if the attacker attacks a node i, the IDS defends node *i*. But if the attacker attacks node j the attacker will do better than before and IDS may not do better. This contradicts the concept of pure NE at Cluster node. Therefore the zero-sum game has no pure NE.
Definition 5: The total cost of intrusion for IDS depends upon the number of attacks on the cluster nodes. The cost also includes the sum of all unsuccessful attacks on each node, with the parameters α, β is

$$I_c = \sum_{i=1}^{N} (\alpha \sum_{j=1}^{m} (\gamma_{i,j}) + \beta N_i)$$

$$where \qquad \alpha + \beta = 1$$

Definition 6: The IDS defends many times for all intruder attacks. For a zero sum game, the cost of the intruder's success and failure attacks equals the cost of success and failures of defending the nodes.
To get a successful attack, an intruder must attack a number of times unsuccessfully. The waiting time for unsuccessful attacks is added to successful attacks of the intruder cost. The profit of the attacker depends upon the number of nodes compromised, but the total cost or energy used by the intruder to compromise the cluster nodes is the sum of the successful and failure attempts.
Theorem 3: In zero sum game, the energy used to defend a cluster is finite.
Proof: The total cost to defend a cluster C_c is the energy spent for successful attempts plus the energy spent for unsuccessful attempts. Therefore C_c is given by

$$C_c = \sum_{i=1}^{N} (\alpha E_c + \beta N_i)$$

$$C_c = \sum_{i=1}^{N} (\alpha (\sum_{j=1}^{m} P_{i,j}) + \beta N_i)$$

Where $\sum_{i=1}^{N} P_{i,j}$ is the energy to defend cluster head E_c is the probability of defending a cluster (equation (2))
Since N is finite, α+β=1 , the number of attempts by an intruder is finite, the energy spent by IDS to defend a cluster is also finite. This concludes the Theorem 3.
The Theorem 3 will further conclude from the equations (7) and (8). According to zero sum game the equations (7) and (8) must be equal. That is
$I_c= C_c$ --- (9)
Substituting for I_c and C_c we get

$$\sum_{i=1}^{N} (\alpha \sum_{j=1}^{m} (\gamma_{i,j}) + \beta N_i) == \sum_{i=1}^{i=N} (\alpha (\sum_{j=1}^{m} P_{i,j}) + \beta N_i) \text{ --- (10)}$$

The above equation concludes that energy spent for number of unsuccessful attempts by intruder equates the energy spent to defend the nodes.

In the selective forwarding attacks, the malicious nodes behave like normal nodes and drop the packets. Identifying such malicious nodes and eliminating them from the data transfer path is very important.
Corollary: The energy spent by IDS at malicious node and normal functional node is null. If a node is compromised, then the node is ill functional and will not be part of the sensor network. The IDS does not have

any effect on such a node. Similarly, if a node is never attacked by an intruder, the IDS will not be activated and therefore no energy is spent. Therefore, the energy spent by IDS at malicious node or non-attacked node is zero (null).

C. Detection of malicious node

In the intrusion detection problem, IDS needs to protect each cluster in the network. Since we are considering one cluster at a time, detection of a malicious node on the path of data flow is very important. We assume that the network is operating under ideal radio conditions. consequently, packet loss appears due to malicious activity. In the current zero sum game, the IDs and intruders are non-cooperative players. The intruder maximizes its benefits by destroying the functionality of the system and the protector tries to protect the facility. In this research, our problem is to detect malicious node in the forward path. In the sensor communications path, total number of acknowledgements expected to receive at the source equals sum of the acknowledgements received and acknowledgements dropped.

CONCLUSIONS

One of the methods used to detect the malicious node in the forward attack is authentication for multi-hop acknowledgement-based detection. In the proposed scheme, we selected one or more intermediate nodes along the forwarding path to determine the malicious node (s).

The random check points are selected to detect the malicious node in the communications path using zero sum game. The zero sum game presented in the current model shows the total energy required is constant. Thus game theory plays an important role in detection of false node in WSN.

REFERENCES

[1] Altman, A.; Bercovici-Boden, A.; and Tennenholtz, M. 2006. Learning in one-shot strategic form games. In ECML, 6–17.

[2] Camerer, C.; Ho, T.; and Chong, J. 2001. Behavioral game theory: Thinking, learning, and teaching. Nobel Symposium on Behavioral and Experimental Economics.

[3] Camerer, C.; Ho, T.; and Chong, J. 2004. A cognitive hierarchy model of games. QJE 119(3):861– 898. Camerer, C. F. 2003. Behavioral Game Theory: Experiments in Strategic Interaction. Princeton University Press.

[4] Chong, J.; Camerer, C.; and Ho, T. 2005. Cognitive hierarchy: A limited thinking theory in games. Experimental Business Research, Vol. III: Marketing, accounting and cognitive perspectives 203–228

[4] Chris Karlof and David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, First IEEE International Workshop on Sensor Network Protocols and Applications, 2003

[5] Krontiris Ioannis, Tassos Dimitriou, and Felix C. Freiling, “Towards Intrusion Detection in Wireless Sensor Networks”, EuropeanWireless Conference, Paris, April 2007

[6] kuldeep, K. Sharma, and M. K. Ghose, “Wireless Sensor Networks Security: A New Approach”, DCOM 2008, Dec14-17, 2008.

[7] Roman, R. Jianying Zhou Lopez, J., Applying intrusion detection systems to wireless sensor networks, 3rd IEEE Consumer Communications and Networking Conference, 2006. CCNC 2006.

[8] Vijay Bhuse, Ajay Gupta, “Anomaly intrusion detection in wireless sensor networks”, Journal of High Speed Networks, Volume 15, Issue 1, January 2006.

[9] Michael Krishnan, “Intrusion Detection in Wireless Sensor Networks”,walrandpc.eecs.berkeley.edu/228S06/Projects/KrishnanProject.pdf

[10] A. Agah, S. K. Das and K. Basu, “A game theory based approach for security in wireless sensor networks”, IEEE International Conference on Performance, Computing, and Communications, 2004.

[11] A. Agah, S. K. Das and K. Basu, “A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks”, Vehicular Technology Conference (VTC2004), Fall 2004.

[12] A. Agah, K. Basu and S. K. Das, “Preventing DoS attack in Sensor Networks: A Game Theoretic Approach”, IEEE International Conference on Communications (ICC 2005), Volume 5, Issue , 16-20 May 2005

[13] Michael Brownfield, “Wireless Sensor Network Denial of Sleep Attack”, Proceedings of the 2005 IEEE Workshop on Information Assurance and Security”, United States Military Academy, West Point, NY.

[14] R. Negi and A. Perrig, “Jamming analysis of MAC protocols”, Carnegie Mellon Technical Memo, 2003.

[15] A. B. MacKenzie and L. A. DaSilva, “Game Theory for Wireless Engineers”, Synthesis Lectures on Communications, 2006. Morgan & Claypool Publishers.

[16] A. Agah, “A Novel Game Theoretic Framework for Security in Wireless Sensor Networks”, Ph. D Thesis, UT Austin, December 2005.

[17] T. Alpcan and T. Basar, “An intrusion detection game with limited observations,” in 12th Int. Symp. on Dynamic Games and Applications, Sophia Antipolis, France, July 2006.

[18] M. Kodialam, T.V. Lakshman, “Detecting network intrusions via sampling: a game theoretic approach”, Proceedings of Twenty Second IEEE INFOCOMM, 2003.

[19] S. Zhu, S. Setia, and S. Jajodia, “LEAP : efficient security mechanisms for large-scale distributed sensor networks”, Proceedings of the 10th ACM conference on Computer and Communication Security, Washington D.C., 2003.

[20] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks”, Proceedings of the 9th ACM conference on Computer and Communications Security, Washington, DC, USA, 2002.

[21] J. R. Douceur, “The Sybil Attack”, First International Workshop on Peer-to-peer Systems, LNCS 2429, 2002.

[22] J.-H. Yun, I.-H. Kim, J.-H. Lim, and S.-W. Seo, “WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks”, Ubiquitous Convergence Technology, ICUCT, 2006.

[23] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks”, Computer, 35(10), 2002.

[24] M. Kim, I. Doh, and K. Chae, “Denial-of-Service(DoS) Detection through Practical Entropy Estimation on Hierarchical Sensor Networks”, The 8th International Conference Advanced Communication Technology, (ICACT 2006), 2006.

[25] A. Agah, S. K. Das, K. Basu, and M. Asadi, “Intrusion Detection in Sensor Networks: a Non-Cooperative Game Approach”, Proceedings of Third IEEE International Symposium on the Network Computing and Applications (NCA’04), IEEE Computer Society, 2004.