NON-ZERO SUM GAME THEORY IN LOCALIZING A FALSE NODE IN WSN

Dr. Sridevi Kotari,
Assistant Professor, CSE, Muffakham Jah College of Engineering & Technology, Hyderabad, Telangana, India.
devijak@gmail.com

Depangi Ravi,
Assistant Professor, CSE, School of Technology, GITAM Hyderabad, Telangana, India
ravi.depangi@gmail.com

Srinivasa Rao Dhanikonda,
Assistant Professor, CSE, School of Technology, GITAM Hyderabad, Telangana, India
srinivasarao.dhanikonda@gmail.com

Srisailapu D Vara Prasad,
Assistant Professor, CSE, School of Technology, GITAM Hyderabad, Telangana, India
sdvprasad554@gmail.com

Abstract: Since WSN become wide spread, safety becomes a cardinal event. Wireless sensor networks has developed a good deal in the past several years and provides excellent chances in defense related programs like tracking surroundings and collecting information linked to antisocial actions. Right now, the requirements of wireless detectors have become inescapable in everyday life. With the constant development of Wireless sensor networks daily life, organization, and protection programs, the safety of transferring information from detectors to their destination is now an important research field. As a result of constraints of electricity, storage, and processing capacities, present security mechanics of wireless networks or wired systems can't use directly into wireless sensor systems. So there's a requirement to come up with new tactics or alter the present security mechanisms to move information from source (in the area) to base channel (destination). Within this paper we discuss now available intrusion detection methods, assault versions with game theory, and then propose a new frame to discover malicious nodes with zero sum game strategy for nodes at the forward data path. The very first portion of study stipulates the sport version with probability of electricity necessary for shifting the information packets. The second section derives the version to discover the malicious nodes with likelihood of acknowledgement at source.

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

I. Introduction

The exceptional qualities of sensor networks restrict the applicability of conventional safety measures. Since sensor nodes have limited power resources, limited community memory and calculation capability, they aren't able to save long-sized keys or operate complicated cryptology algorithms. Normally sensor nodes are deployed, and might not have a worldwide identification number due to the massive quantity of overhead. They might also fail because of lack of electricity or physical harm. The dynamic character of sensor networks' topology is generally because of node failure or node insertion rather than node mobility because most sensor networks programs don't presume an extremely cellular attribute. The majority of the programs of those WSNs are still all unattended. The WSNs installation area might be impossible to strategy, because the environment can be dangerous and hostile. Therefore,

WSNs have to be sovereign and display responsiveness and adaptability for development changes in actual time. Because of such reasons, the system operation demands proper administration to obtain the data. The autonomous character of WSN nodes along with their restricted funds makes them vulnerable to attacks. To supply normal performance of those WSN nodes, then we have to offer some mechanism inside the community itself. The Traditional security methods can't be utilized right in WSNs Due to following special attributes: The low cost and resource restrained in terms of energy, memory, computation, and communication Capabilities. They may be deployed in public hostile locations, where they are vulnerable to physical attacks by adversaries. The hackers may take control of sensor nodes and extract secret information. Due to basic properties of the nodes, they may be dynamically reorganized and use insecure communication

Because of this, existing safety mechanisms are insufficient, and new strategies are wanted. WSNs are exposed to a lot of attacks due to broadcast character of transmission moderate, source restriction on sensor nodes, and uncontrolled environments where they're left unattended. Comparable to other communication methods, WSNs possess the next overall safety aims.

II. Security objective

When dealing with security, one is faced with achieving some or all of the following goals are Availability, Authenticity, Freshness, Data Integrity, and Scalability. Which are described as follows: Suggests that the information is current and guarantees no adversary replayed older messages. It Resources are readily available to approved parties when required along with the sensor system must ensure the survivability of community services despite refusal of some service (DoS) attack. To make sure the access to message security, the sensor system must also guard its sources to minimize energy intake. Networks can't use a keying strategy which has poor scaling properties in Space or power necessary to send messages from 1 node to another won't be known beforehand. Network Terms of energy expenditure or latency. Generally, the Amount of acquaintances and the Adversary may easily intercept messages, or so the recipient should be certain the information utilized in almost any decision-making procedure arises from a trustworthy source. A private message is resistant into showing its significance to an eavesdropper. Confidentiality ought to be offered by keys as little a range as possible, to dissuade one break from undermining a massive section of the network.

III. Game Theory

Game theory is a sophisticated branch of smart optimization. The version of game theory reflects a match between players classes which choose to act cooperatively or non-cooperatively and attempt to advertise their rewards (payoffs) throughout the used system (ies) implemented through the accumulative players activities. Research the basic definitions of sport parameters, which may be outlined as follows: 1. A sport is an outline of this strategic interaction between opposing, or even Dealing, pursuits where the limitations and payoff for activities have been taken under account. A participant is a simple thing in a sport, which can be included in the sport using a restricted set of gamers denoted by N that's accountable for shooting logical activities, denoted by Ai, for every player. A player can represent a individual, machine, or group of individuals inside a match. The Utility/Payoff is the positive or negative reward to a player for a given action within the game denoted by ui : $A \rightarrow R$, which measures the outcome for player i determined by the actions of all players $A = \in X$ Ai Ni where the symbol X denotes Cartesian product. A strategy is a plan of action within the game that a given player can adopt during game play denoted by a strategic game

N((A),(u_i)). 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. Nash equilibrium is a profile of optimal actions ∗a A ∈ such that any player ∈i 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}*)≥ (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.

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,

$$\sum_{i=1}^{2} ui(s) = 0 \forall s \in S$$

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.

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.

Games Theory for WSNs Security: The various game types which are generally utilized to simulate WSNs security problems can be categorized to combined games and non-cooperative games as exhibited. The combined games have been represented by working nodes aiming at optimizing the entire networks safety against different safety hazards. To the contrary, the non-cooperative matches demand the contradictory individual activities for which each node aims at optimizing its payoff which opposes others' results. Figure 1 lists the different Kinds of matches Which Have Been used to simulate security issues in WSNs (Figure 1 doesn't exhibit a classification for games Generally, but presents that the most matches Which Have Been utilized in the literature to simulate WSNs safety issues

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

$$\text{Cc} = \sum_{i=1}^{N} \partial Ec + \beta Ni$$

$$\text{Cc} = \sum_{i=1}^{N} \partial (\sum_{j=1}^{m} pij) + \beta Ni$$

Where , $\sum_{j=1}^{m} pij$ is the energy to defend cluster head Ec 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.

That is Ic= Cc

Substituting for Ic and C c we get

$$\sum_{i=1}^{N}(\alpha \sum_{j=1}^{m}(\gamma\, i,j) + \beta Ni == \sum_{i-1}^{N}(\alpha(\sum_{j=1}^{m} Pi,j) + \beta Ni)$$

The aforementioned equation concludes the energy spent for variety of unsuccessful efforts by intruder equates that the energy invested to shield the nodes. From the specific forwarding strikes, the lymph nodes behave as regular nodes and discard the sticks. Discovering such malicious nodes and removing them in the information transfer route is essential.

Due to malicious node From the intrusion detection issue, IDS should safeguard each bunch from the community. Since we're considering one audience at one time, discovery of a malicious node on the route of information flow is essential. We suppose that the system is working under ideal radio conditions. Therefore, packet loss seems because of malicious action. The intruder exerts its advantages by ruining the performance of this machine and also the shield attempts to safeguard the centre. Within this study, our difficulty is to discover malicious node from the forward route. From the detector communications route, total amount of acknowledgements anticipated to get in the origin equals amount of their acknowledgements obtained and acknowledgements fell. The power by IDS at malicious node and ordinary practical node is null. In case your node is compromised, then the node is ailing functional and won't be a part of the detector system. The IDS doesn't have any impact on this a node. In the same way, if your node is not assaulted by an intruder, then the IDS won't be triggered and therefore no electricity is invested.

IV. Conclusion

Among the approaches used to discover the malicious node from the forward assault is authentication for multi-hop acknowledgement-based detection. In the proposed strategy, we picked a couple of intermediate nodes along the forwarding route to find out the malicious node (s). The random test points are chosen to discover the malicious node from the communications route utilizing zero sum game. The zero sum game introduced in the present version indicates the whole energy needed is continuous. Thus game concept plays an Significant role in discovery of fictitious node in WSN.

V. 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.

[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.