Asian Journal of Information Technology 15 (4): 825-832, 2016
ISSN: 1682-3915

Secure Cluster-Based Routing Scheme for Wireless Sensor Networks Using Bargaining Game Model

R. Velayutham
Department of Computer Science and Engineering,
Einstein College of Engineering, Tamil Nadu, India

Abstract: Game theory is a mathematical framework that describes the occurrence of conflict and cooperation between decision makers. Recently, game theory provides an insight into approaches for optimization to enhancing security for Wireless Sensor Networks (WSNs). Reaching an agreement becomes an optimization problem in clustering process. Players in a bargaining problem bargain for the objective as a whole at a particular instant. The problem divided into parts of the whole objective become subject to bargaining during different stages. Each player prefers to reach an agreement in these games. A player with an agreement alone allowed to clustering process. Otherwise, a player who not reaches an agreement is considered as malicious. This scheme is not allowed the malicious nodes to participate in clustering process. Bargaining solution is involved while each player agreement favour their interest. In bargaining game theory, individual player make their decisions is sufficient for predicting an agreement results in providing efficient clustering process in WSNs. An agreement has been represented by utility function.

Key words: Bargaining game, clustering, malicious nodes security, wireless sensor networks, malicious nodes

INTRODUCTION

The characteristics of WSNs are desirable features for various application areas for remote sensing, detecting, tracking and monitoring. Wireless networks force the security challenges to network designers that degrade the network performance. Various attacks are vulnerability by arbitrarily neglecting to route some messages. It is very much essential to design the WSNs to achieve objectives such as maximum coverage of field with help of clustering. Game theory approaches play a vital role in cluster based routing (Koltsidas and Pavlidou, 2011; Hu and Shen, 2010) and network design (Kim, 2014) in Ad-hoc networks. In order to achieve malicious-free WSNs, Game theory (Machado and Tekinay, 2008) is a pretty solution to accomplish the security design. Game theory (Shi *et al*., 2012) describes the behavior of players in a game. Players may be either cooperates or non-cooperative while motivates to maximize their outcomes in the game. The WSNs security (Shen *et al*., 2011) is challenging duo to limited capabilities of sensors. The attack-defend in WSNs security solved by game theory in which interactions among strategies of players. A malicious node in WSNs drops messages while involving dynamic routing process. Such a node should be neglect from the networks to improve the packet delivery ratio. Recently, various game theory models such as non-cooperative game model (Dai *et al*., 2011). Evolutionary game-based data aggregation model (Lin *et al*., 2011; Ma and Krings, 2011) and repeated-game theory of cooperative model (Liu *et al*., 2010) are applied to enhance energy-efficiency (Mehta and Kwak, 2010), power control (Sengupta *et al*., 2010), packet forwarding (Zhao and Shi, 2010) and improving cooperation (Ng and Seah, 2010).

We use bargaining game model for the purpose of ensuring security in WSNs. It optimizes sensor's decision making process in forwarding data packets when they received. The goal of the bargaining game theory provides an optimal strategy for reaching an agreement in clustering process. We design a Secure Cluster-based Routing Scheme using Bargaining Game model (SCRS-BG) in WSNs for enhancing secure routing. Its goal is to prevent malicious node in involving forming cluster process in the network. Differently, from the above literature schemes, this research reveals the best outcome to reduce activities of malicious nodes. The contributions of this research are summarized as follows: first, we formulate the bargaining game for clustering problem statement in the network. To use axiomatic approach for finding, the best outcome of the strategic profile for reach an agreement. Then, Nash bargaining solution is used to solve the optimization problem related to players reached an agreement in the clustering process. Through extensive simulation results, we evaluate the performance of the proposed SCRS-BG. The results show that the SCRS-BG outperforms in terms of detection accuracy and success defense rate.

Literature review: Security is a key parameter in WSNs for remote environments that cause various threats to consistent network operation. In general, a node that acts selfishly drops the packets to degrade the network performance. It is essential to selfish nodes need to be isolated from the networks with low reputation. Game theory approaches (Renita and Sirin, 2008) can be applied to optimize network performance by exploiting the distributed decision making capabilities of WSNs. Game theory (Barcelo *et al*., 2011) has been applied in contention free schemes to consume energy by diminishing collisions.

Malawski (2013) and Asadi *et al*. (2013) proposed a Game-Theoretic Approach to Security and Power Conservation (GT-SPC) in WSNs. Nodes in WSNs accomplish the optimization their decision making based on game theory. Defining a suitable cost and profit to routing and forwarding incoming packets and keeping a history of experiences with non-cooperating nodes drives malicious nodes out of the wireless sensor network. Boudia *et al*. (2015) proposed a homomorphic encryption scheme and aggregate MAC to provide the end-to-end confidentiality and integrity. The scheme employs stateful public key encryption to provide an efficient security. This scheme does not enforce any bound on the aggregation function. Security risk (Jirasek, 2012) is an area that is constantly moving to respond to new threats, standards and technologies.

Kaliappan and Paramasivan (2015) used a dynamic bayesian signalling game to reveal the best actions of individual strategy to minimize the utilities of malicious nodes in MANETs by analyzing strategy profiles for regular and malicious nodes. used a belief-updating system to update a node's belief in terms of action chosen, message sent and strategy chosen. A regular node in the network periodically follows the belief-update process for its private information; it then chooses a probability to cooperate with its neighbouring node.

Xu *et al*. (2013) proposed game-theory based clustering approach for WSNs. A game-theoretic model is built for Cluster Head (CH) selection. This scheme adopts data replication to reduce possible network disconnection. The selection of a candidate CH is discussed under a second price sealed auction. Agah *et al*. (2006) proposed a scheme for detecting passive Denial of Service (DoS) attacks by malicious nodes in the network. The researchers surveyed game theory mechanisms at the network layer between malicious nodes that do not forward other packets and an intrusion detector residing at the base station. Malicious nodes in this research are those nodes that selfishly do not forward incoming packets. The game formulations in (McCune *et al*., 2005) where an attacker turns nodes malicious and prevents them from letting broadcast messages reach other nodes in the network. The intrusion detector monitors WSN of N nodes and detects attacks by malicious nodes by keeping track of collaboration of nodes which accumulates into reputation ratings for a node over time. They model this scenario as a repeated game where the IDS use the history of nodes' collaboration to determine paths comprising of malicious nodes. The game is played as a non-cooperative N-player game between N nodes in the WSN and an IDS residing at the BS. Antoniades *et al*. (2003) introduced local max with no overlap algorithm to strategies for improvement of Pursuit-evasion games. The performance of the local-max and global-max strategies can be improved by avoiding overlap between the sensing regions of pursuers. This reduction in incentives forces pursuers to choose strategies to move to un-sensed locations to detect the evaders.

Shamshirband *et al*. (2014) proposed cooperative Game Theory-based Fuzzy Q-Learning (GT-FQL) for WSNs. It is a three player strategy game consisting of sink nodes, a base station and an attacker. The game performs at any time a victim node in the network receives a flooding packet as a DoS attack beyond a specific alarm event in WSNs. Zhu *et al*. (2012) described a collaborative intrusion detection system to analyze an incentive based resource allocation problem. It needs enough credits to detect malicious nodes, otherwise, it drops the packets. Markus studied an infinitely repeated discounted game in which a player perfectly observes any other player's action choice with a fixed and finite delay. This game has no pure strategy Nash Equilibrium. Marcin introduced a procedural value for cooperative games to determine the sharing marginal contributions to coalitions that formed by players joining in random order. It allows false data injection into networks by compromised insiders eavesdropping data transmission.

Hameed and Slinko (2015) characterized roughly weighted hierarchical games. It used secure secret sharing schemes to be defined on these games as access structures. It shows that hierarchical games are rather far from weighted and even roughly weighted games. Shapley value is used as a solution of the cooperative allocation game. Hao *et al*. (2014) proposed a Joint Channel Allocation and Power Control Game model that considered a best response strategy to improve the convergence speed in the network. Balkenborg *et al*. (2015) presented the refined best-response correspondence of a game. This scheme is derived from the original game by reducing the payoff by a small amount for all pure strategies that are weakly inferior.

Weakly inferior strategies for two-player games are pure strategies that are either weakly dominated or are equivalent to a proper mixture of pure strategies. Fixed points of the refined best-response correspondence are not equivalent to any known Nash equilibrium refinement. A class of simple communication games demonstrates the usefulness and intuitive appeal of the refined best-response correspondence. Miao and Xu (2013) presented cooperative coalitional game that provides a power control solution based on the trade-off between energy efficiency and end-to-end delay. This scheme achieves a fair distribution of the total cost among sources. It is observed that the additional energy cost function and the delay cost function are continuously differentiable. Each source node seeks to minimize, its utility function of discounted sum of transmission power increase cost and source-to-sink delay cost. Anithaashri and Baskaran (2012) determined the action for a player in multi-player game environment with the mixed strategy. The utility function can be obtained with the player's preferences over the game of possible outcomes while the problem is a game with mixed strategies. Finally, the Nash equilibrium is computed and best-response strategies for the players such as administrator and attacker are found.

MATERIALS AND METHODS

The clustering in WSN is described as bargaining problems that represent situations in which there is a conflict of interest about agreements, individuals have the possibility of concluding a mutually beneficial agreement and no agreement may be imposed on any individual without his approval. In this approach, the sensor node who involved in forming cluster must reach an agreement that is formulated by a bargaining game approach. We assume that nodes with not reach an agreement is considered as malicious. The strategic or non-cooperative mechanism entails clearly modeling the bargaining game process.

A bargaining game is formulated as BG = <n; a; u > where ni is the set of decision makers (sensor nodes), ai is the player's action and {ui} is the utility functions that each player i wishes to maximize.

Bargaining model allows two players to offer alternating proposals indefinitely and it assumes that future payoffs of players 1-2 are discounted by δ_1, $\delta_2 \epsilon (0, 1)$. It provides alternate offers for stationary xstrategy profile that is a sub-game perfect equilibrium for this game. The δ_1 is the discount factor. Player 1 proposes and accepts offer y if and only if, $y \geq y_1 \geq$. Player 2 proposes and accepts offer x if and only if, $x \geq x_1$:

$$x_1 = \frac{1-\delta_2}{1-\delta_1\delta_2}, y_1 = \frac{\delta_1(1-\delta_2)}{1-\delta_1\delta_2} \quad (1)$$

$$y_1 = \frac{\delta_1(1-\delta_1)}{1-\delta_1\delta_2}, y_1 = \frac{(1-\delta_2)}{1-\delta_1\delta_2} \quad (2)$$

It clearly shows that an agreement is reached immediately for any values of δ_1 and δ_2. To gain more insight into the resulting allocation, assume for simplicity that. If player 1 moves first, the division will be 1/1+δ, δ/1+δ and if player 2 moves first, the division will be δ/1+δ, 1/1+δ. The Frst Mover's Advantage (FMA) is clearly related to the impatience of the players related to discount factor. Now, the discount factor is derived from some interest rates r_1 and r_2. If δ->1, the FMA disappears and the outcome tends to (1/2, 1\2) If δ-> 0, the FMA dominates and the outcome tends to (1, 0):

$$\delta_1 = e^{-r_1\Delta t}, \delta_2 = e^{-r_2\Delta t} \quad (3)$$

Equation 3 represents a continuous-time approximation of interest rates. It is equivalent to interest rates for very small periods of time Δt:

$$e^{-r_1\Delta t} = \frac{1}{1+r_i\Delta t} \quad (4)$$

The Δt-> 0 influence to get rid of the first mover's advantage:

$$\lim_{\Delta t\to 0} x_1 = \lim_{\Delta t\to 0} \frac{1-\delta_2}{1-\delta_1\delta_2} = \lim_{\Delta t\to 0} \frac{1-e^{-r_2\Delta t}}{1-e^{-(r_1+r_2)\Delta t}} \quad (5)$$

In bargaining game model, an axiomatic approach is used to involve the details process of bargaining and considers only the set of outcomes or agreements that satisfy "reasonable" properties.

For example, suppose 2 players must split one unit of a good. If no agreement is reached then players do not receive anything. Preferences are identical. It is expected to players to agree or pareto efficiency and each to obtain half or symmetry. This scheme use X to denote set of possible agreements and D to denote the disagreement outcome. It general scenario is expressed as follows:

$$X = \left\{(x_1, x_2) | x_1 + x_2 = 1, x_i \geq 0\right\}, D = (0,0) \quad (6)$$

Pareto efficiency of bargaining solution f (U, d) is Pareto efficient if there does not exist a $(V_1, V_2) \in U$ such that $V \geq f(U, d)$ and $V_i \geq f_i(U, D)$ for some i. An inefficient outcome is unlikely, since it leaves space for renegotiation. Symmetry of bargaining solution (U, d) be such that $(V_1, V_2) \in U$ if and only if $(V_1, V_2) \in U$ and d1 = d2. Then $f_1(U, D) = f_2(U, D)$ If the players are indistinguishable, the agreement should not discriminate between them. Each player i has preferences that represented by a utility function u_i over $x \cup d$. The set of possible payoffs by set U defined by:

$$U = \left\{ (v_1, v_2) \middle| u_1(x) = v_1, v_2(x) = \right\} \quad (7)$$

$$v_2 \text{ for some } x \in X$$

$$d = \left(u_1(D), u_2(D)\right) \quad (8)$$

A bargaining problem is a pair (U, d) where $U \cup R^2$ and $d \in U$. We assume that U is a convex and compact set. There exists some $v \in U$ such that $v > d$ ($v_i > d_i$ for all i). Utility functions are only representation of preferences over outcomes. A transformation of the utility function that maintains the some ordering over preferences such as a linear transformation should not alter the outcome of the bargaining process.

Nash bargaining solution: Nash bargaining solution solves the optimization problem related to players reached an agreement in the clustering process. A pair of payoffs (v1, v2) is a Nash bargaining solution to solve the optimization problem. It expressed by Eq. 9:

$$\max_{v_1, v_2} (v_1 - d_1)(v_2 - d_2) \text{ Subjected to} \quad (9)$$
$$(v_1, v_2) \in U, (v_1, v_2) \geq (d_1, d_2)$$

The Nash bargaining solution is denoted by f^N (U, d). An optimal solution exists in set U that compact and the objective function of problem is continuous. The objective function of problem is strictly quasi-concave that represents a unique optimal solution. Nash bargaining solution f^N (U, d) is the unique bargaining solution that satisfies the 4 axioms.

Proof: The proof has 2 steps. We first prove that Nash bargaining solution satisfies the 4 axioms. We then show that if a bargaining solution satisfies the 4axioms, it must be equal to f^N (U, d).

Step 1; Pareto efficiency: This follows immediately from the fact that the objective function of problem is increasing in v_1 and v_2.

Symmetry: Assume that $d_1 = d_2$. Let $v = (v_1, v_2) = f^N(U, d)$ be the Nash bargaining solution. Then, it can be seen that (v_2, v_1) is also an optimal solution of that problem. By the uniqueness of the optimal solution, we must have $v_1 = v_2$, therefore, $f_1^N(U, d) = f_2^N(U, d)$.

Independence of irrelevant alternatives: Let $U \subseteq U$. From the optimization problem characterization of the Nash bargaining solution, it follows that the objective function value at the solution f^N (U, d) is greater than or equal to that at f^N (U, d). If $f^N(U, d) \in U$, then the objective function values must be equal, It reveals that the f^N (U, d) is optimal for U and by uniqueness of the solution f^N (U, d = f^N (U, d)). Invariance to equivalent payoff representations provides f^N (U, d) that is an optimal solution of the problem.

Step 2: Let f (U, d) be a bargaining solution satisfying the 4 axioms. We prove that $f(U, d) = f^N(U, d)$. Let $z = f^N(U, d)$ and define the set:

$$U' = \left\{ a'\upsilon + ß \,|\, \upsilon \in U; a'z + ß = \left(\frac{1}{2}, \frac{1}{2}\right); a'd + ß = (0, 0)' \right\} \quad (10)$$

We map the point z to (1/2, 1/2) and the point d to (0, 0). Since, f (U, d) and f^N (U, d) both satisfy axiom 3 (invariance to equivalent payoff representations), we have $f(U, d) = f^N(U, d)$ if and only if $f(U, 0) = f^N(U, d) = (1/2, 1/2)$. Hence to establish the desired claim, it is sufficient to prove that:

$$f(U, 0) = \left(\frac{1}{2}, \frac{1}{2}\right) \quad (11)$$

Since U' is bounded, we can find a rectangle U' symmetric with respect to the line $v_1 = v_2$ such that $U' \subseteq U''$ and (1/2, 1/2) is on the boundary of U''. By Axioms 1 and 2, f (U'', 0) = (1/2, 1/2). By Axiom 4, since $U' \subseteq U''$, we have f (U', 0) = (1/2, 1/2) completing the proof.

The variant of the bargaining game with alternating offers with and Nash's axiomatic model yield the optimal outcome. A node with not reaching an agreement is prevented in clustering process to enhance the network security.

RESULTS AND DISCUSSION

The proposed scheme has been implemented in Network Simulator (NS2). The main objective of the simulation was to enhance security in the clustering process that prevents the malicious nodes. About 200

sensor nodes were randomly deployed in a 1000×1000 m area of interest. The transmission range was 20 m. The proposed SCRS-BG scheme forms the malicious-free clusters in WSN to enhance the security.

The performance of the proposed scheme was evaluated by comparing, it with the related GT-FQL and GT-SPC schemes in terms of utility, packet drop ratio, detection accuracy, number of alive nodes and cluster overhead. The simulation results were studied by varying the percentage of malicious nodes from 10-50% that may caused packet drop attack and false claim. The GT-FQL and GT-SPC schemes are aimed to enhance security by using fuzzy learning with game theory approach and security and power conservation system, respectively. The proposed SCRS-BG used bargaining game solution that integrated with axiomatic mechanism to involve the details process of bargaining and considers only the set of outcomes or agreements that satisfy "reasonable" properties. It prevents packet drop attack and false claim attack. This is significantly helpful to properly confine the malicious nodes in the network. The proposed SCRS-BG scheme can effectively find and detect the different anomalies like packet drop attack and false claim attack in WSNs.

Packet drop ratio: Figure 1 shows the packet drop rates over the simulation time. We see that as time goes on, the packet drop rates of the related schemes GT-FQL and GT-SPC. The proposed SCRS-BG performed on less packet drop ratio because, it uses bargaining solution to prevent malicious nodes reach an agreement. This is because the strategy ensures that the nodes in SCRS-BG gain higher payoff. The GT-SPC has no defense mechanism to encourage cooperative behaviors and punish the nodes with false claim to participate in clustering process. The proposed SCRS-BG maintained lower packets drop ratio because false claim nodes in entire clustering process are not allowed for routing where as the GT-FQL and GT-SPC achieved higher packet drop about 29 and 40%, respectively. Figure 2 clearly shows that the proposed SCRS-BG takes less time to detect the malicious node.

Utility: Utility represents the number for every possible outcome of the player that motivates the players involving better cooperation among others and prevent false claim in clustering process. Utility functions are only representation of preferences over outcomes that prevent dropping packets in routing process. In any situation at least one player is able to maximize the expected payoff through anticipating the responses to its actions. In SCRS-BG scheme, players are indistinguishable and the

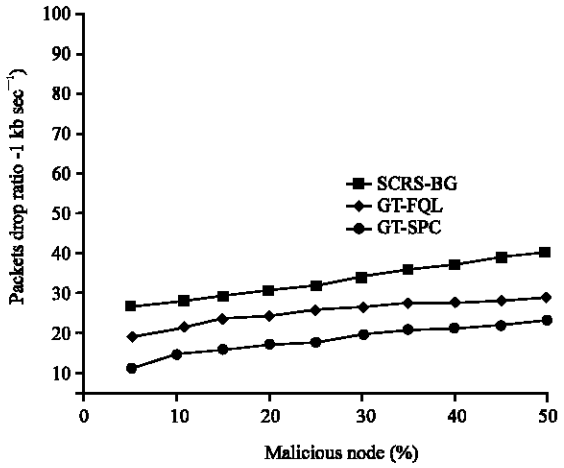

Fig. 1: Packets drop ratio

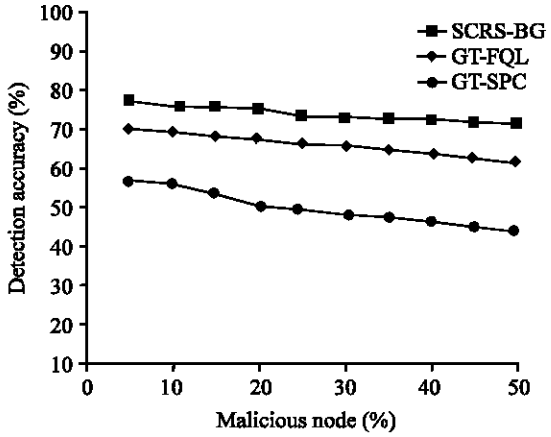

Fig. 2: Utility of nodes

agreement should not discriminate between them. Figure 2 show that the proposed SCRS-BG scheme has more utility about 88% that maximize the cooperation among the nodes. The related schemes GT-FQL and GT-SPC have less utility value that shows they did not perform well in the presence of malicious nodes and they cannot choose a route to forward packets for others.

Figure 2 clearly noticed that a node's utility is high when it follows the bargaining solution. A transformation of the utility function that maintains the some ordering over preferences such as a linear transformation should not alter the outcome of the bargaining process. This is because nodes get more chance to reach an agreement to make clusters.

Detection accuracy: Figure 3 shows the detection accuracy of proposed SCRS-BG and related schemes GT-FQL and GT-SPC. It is clearly marked that the SCRS-BG with a Nash bargaining solution satisfies the 4

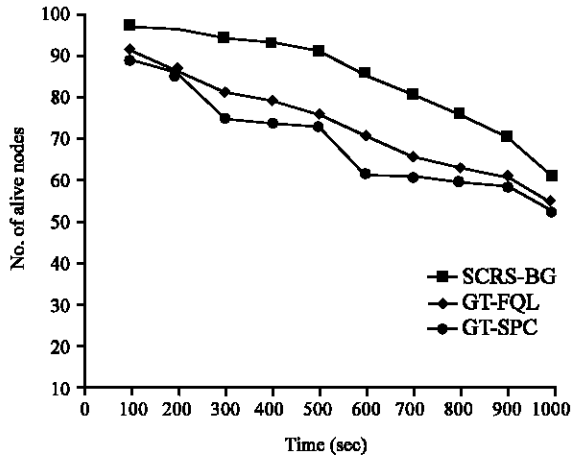

Fig. 3: Detection accuracy

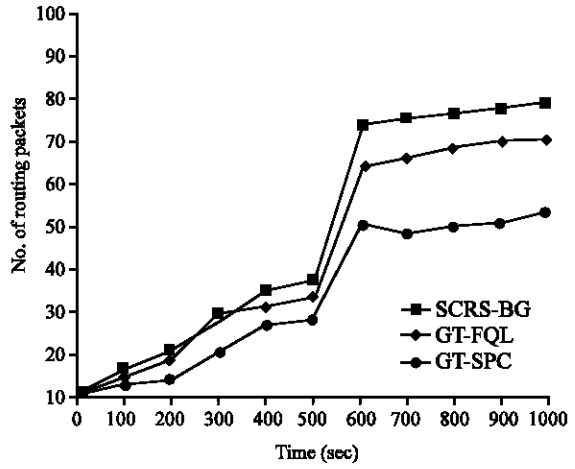

Fig. 4: Number of alive nodes under attack

axioms that provides an optimal solution of the problem of reaching agreement. It can also be inferred that detection accuracy per percentage of attack is higher with the SCRS-BG scheme than the other related GT-FQL and GT-SPC schemes. At higher attack frequencies, the proposed SCRS-BG scheme displays greater accuracy ratio about 75% but the related schemes GFQL and IS-RS/PS has 62 and 45%, respectively because they cannot be detected the malicious node effectively in WSNs.

Number of alive nodes under attack: This experiment was conducted to evaluate the performance of proposed SCRS-BG scheme in terms of number of live nodes during the simulation runtime. In the current run, the number of sensor nodes was 100. Figure 4 displays the number of live nodes for proposed scheme and related schemes

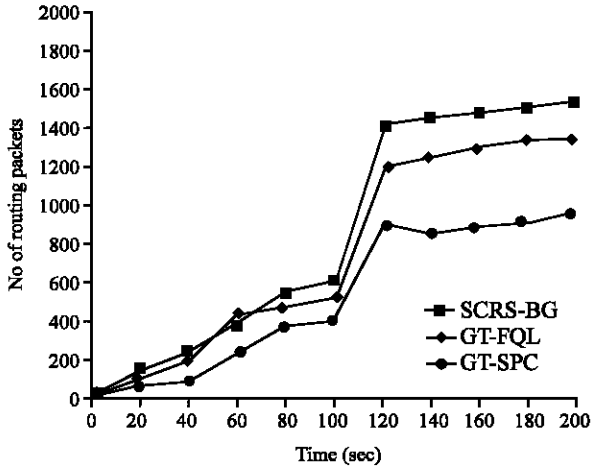

Fig. 5: Cluster overhead

throughout simulation runtime about 1000s. Figure 4 clearly noticed that the number of live sensor nodes in the proposed SCRS-BG method is significantly greater than existing GT-FQL and GT-SPC schemes. However, the proposed method gained the advantage of a successful defense rate due to the higher percentage of malicious nodes detected compared to related schemes. The SCRS-BG maintains 60 live nodes against an attack in comparison to 54 and 52 nodes for GT-FQL and GT-SPC, respectively.

Cluster overhead: In this simulation, the cluster overhead by the proposed SCRS-BG during packet drop attacks and false claim is evaluated. Figure 5 provides the comparison between the proposed SCRS-BG scheme and existing GT-FQL and GT-SPC schemes in terms of number of routing packets (RTP) transferred in clustering process in WSNs. It is noticed that the SCRS-BG maintained lower clustering overhead about 973 RTP while varying the number of nodes. The related GT-FQL and GT-SPC schemes generated higher routing packets about 1360 RTP and 1540 RTP, respectively due to arise of routing overhead because of the number of cooperating players in the report is very large. In order to reduce the clustering overhead, the SCRS-BG used a Nash bargaining solution to provide optimal outcome regarding nodes reaches agreement in clustering process.

Routing latency: Figure 6 shows the routing latency for three protocols when the number of malicious nodes varied. Figure 6 was strong-minded that the performance of the proposed scheme is more efficient than the related GT-FQL and GT-SPC schemes. It was revealed that the routing latency of the proposed SCRS-BG is 37 msec with

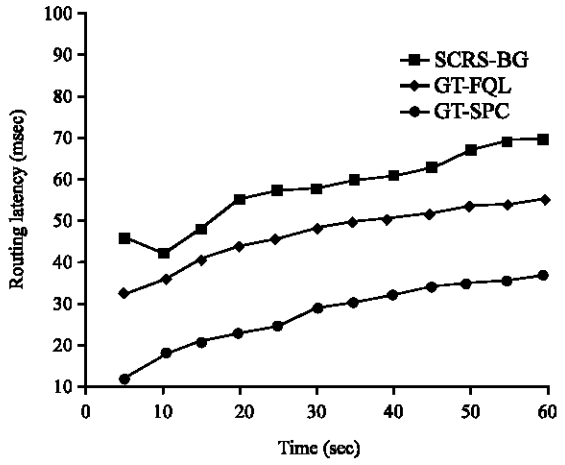

Fig. 6: Routing latency vs. malicious nodes

50% malicious nodes in the network and 55 msec and 70 ms for GT-FQL and GT-SPC, respectively. When simulating a network with 50% malicious nodes, the time taken by the proposed SCRS-BG was 37 msec. The related GT-FQL and GT-SPC schemes took more time for forwarding packets because of more exchanges of routing packets to enhance security. The SCRS-BG uses the Nash bargaining solution in the Bargaining game model to reach an agreement for involving clustering process. Only then does, it allow nodes to send packets to their neighbors with minimal overhead. Therefore, it provides secure routing and enhances the performance of WSNs. Simulation results show that the proposed SCRS-BG exhibits fair detection ability for false claim and provides the better detection performance than related GT-FQL and GT-SPC schemes.

CONCLUSION

In order to enhance secure clustering, we investigated the impacts of applying bargaining game model on accuracy of malicious node detection in WSNs. The bargaining game model incorporated in clustering process with preventions of malicious nodes. In this study, a novel bargaining game model was proposed to encourage nodes to reach an agreement for clustering process. It uses Nash bargaining solution strategy to minimize the false claim of malicious nodes in clustering process in WSNs. The proposed SCRS-BG scheme is resistant to defend against a packet drop attack that enhances the security in WSNs. From the extensive simulation, it has been clearly noticed that individual player make their decisions is sufficient for predicting an agreement to reduce false claim of nodes results in providing efficient clustering process in WSNs. To the best of our knowledge, this is the first research that uses the bargaining game model to prevent false claim and packet drop attack in WSNs. Simulation results show that the proposed SCRS-BG scheme reveals better outcomes than existing schemes. Future research direction is to use this bargaining game approach in power conservation and resource consumption with security.

REFERENCES

Agah, A., M. Asadi and S.K. Das, 2006. Prevention of DoS attack in sensor networks using repeated game theory. Proceedings of the 2006 International Conference on Wireless Networks, June 26-29, 2006, Las Vegas, Nevada, USA., pp: 29-36.

Anithaashri, T.P. and R. Baskaran, 2012. Enhancing the network security using amalgam games. Int. J. Cryptogr. Inform. Security, 2: 25-37.

Antoniades, A., H.J. Kim and S. Sastry, 2003. Pursuit-evasion strategies for teams of multiple agents with incomplete information. Proceedings of the 42nd IEEE Conference on Decision and Control, Volume 1, December 9-12, 2003, Hawaii, USA., pp: 756-761.

Asadi, M., C. Zimmerman and A. Agah, 2013. A game-theoretic approach to security and power conservation in wireless sensor networks. Int. J. Network Security, 15: 50-58.

Balkenborg, D., J. Hofbauer and C. Kuzmics, 2015. The refined best-response correspondence in normal form games. Int. J. Game Theory, 44: 165-193.

Barcelo, J., H. Inaltekin and B. Bellalta, 2011. Obey or play: Asymptotic equivalence of slotted aloha with a game theoretic contention model. IEEE Commun. Lett., 15: 623-625.

Boudia, O.R.M., S.M. Senouci and M. Feham, 2015. A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography. Ad Hoc Networks, 32: 98-113.

Dai, L., Y. Chang and Z. Shen, 2011. A non-cooperative game algorithm for task scheduling in wireless sensor networks. Int. J. Comput. Commun. Control, 6: 592-602.

Hameed, A. and A. Slinko, 2015. Roughly weighted hierarchical simple games. Int. J. Game Theory, 44: 295-319.

Hao, X.C., Q.Q. Gong, S. Hou and B. Liu, 2014. Joint channel allocation and power control optimal algorithm based on non-cooperative game in wireless sensor networks. Wireless Personal Commun., 78: 1047-1061.

Hu, J. and L. Shen, 2010. Clustering routing protocol of wireless sensor networks based on game theory. J. Southeast Univ. (Nat. Sci. Edn.), 40: 441-445.

Jirasek, V., 2012. Practical application of information security models. Inform. Security Tech. Rep., 17: 1-8.

Kaliappan, M. and B. Paramasivan, 2015. Enhancing secure routing in mobile Ad Hoc networks using a dynamic Bayesian signalling game model. Comput. Electr. Eng., 41: 301-313.

Kim, S., 2014. Game Theory Applications in Network Design. IGI Global Publishing Co., Pennsylvania, ISBN: 9781466660519, Pages: 500.

Koltsidas, G. and F.N. Pavlidou, 2011. A game theoretical approach to clustering of ad-hoc and sensor networks. Telecommun. Syst., 47: 81-93.

Lin, J., N. Xiong, A.V. Vasilakos, G. Chen and W. Guo, 2011. Evolutionary game-based data aggregation model for wireless sensor networks. IET Commun., 5: 1691-1697.

Liu, Q., X. Xian, S. Guo and T. Wu, 2010. Repeated-game theory of cooperative model in wireless sensor network routing. Chin. J. Sens. Actuat., 23: 1322-1327.

Ma, Z.S. and A.W. Krings, 2011. Dynamic hybrid fault modeling and extended evolutionary game theory for reliability, survivability and fault tolerance analyses. IEEE Trans. Reliability, 60: 180-196.

Machado, R. and S. Tekinay, 2008. A survey of game-theoretic approaches in wireless sensor networks. Comput. Networks, 52: 3047-3061.

Malawski, M., 2013. Procedural values for cooperative games. Int. J. Game Theory, 42: 305-324.

McCune, J.M., E. Shi, A. Perrig and M.K. Reiter, 2005. Detection of denial-of-message attacks on sensor network broadcasts. Proceedings of the IEEE Symposium on Security and Privacy, May 8-11, 2005, Oakland, CA., USA., pp: 64-78.

Mehta, S. and K.S. Kwak, 2010. An energy-efficient MAC protocol in wireless sensor networks: A game theoretic approach. EURASIP J. Wireless Commun. Networking, Vol. 2010. 10.1155/2010/926420.

Miao, X.N. and G. Xu, 2013. Cooperative differential game model based on trade-off between energy and delay for wireless sensor networks. Ann. Operat. Res., 206: 297-310.

Ng, S.K. and W.K.G. Seah, 2010. Game-theoretic approach for improving cooperation in wireless multihop networks. IEEE Trans. Syst. Man Cybern. B Cybern., 40: 559-574.

Sengupta, S., M. Chatterjee and K. Kwiat, 2010. A game theoretic framework for power control in wireless sensor networks. IEEE Trans. Comput., 59: 231-242.

Shamshirband, S., A. Patel, N.B. Anuar, M.L.M. Kiah and A. Abraham, 2014. Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. Eng. Applic. Artif. Intell., 32: 228-241.

Shen, S., G. Yue, Q. Cao and F. Yu, 2011. A survey of game theory in wireless sensor networks security. J. Networks, 6: 521-532.

Shi, H.Y., W.L. Wang, N.M. Kwok and S.Y. Chen, 2012. Game theory for wireless sensor networks: A survey. Sensors, 12: 9055-9097.

Xu, Z., Y. Yin, X. Chen and J. Wang, 2013. A game-theory based clustering approach for wireless sensor networks. Proceedings of the 2nd International Conference on Next Generation Computer and Information Technology, September 22-24, 2013, Qingdao, China, pp: 58-67.

Zhao, Y.H. and H.S. Shi, 2010. Game theoretical packet forwarding algorithm in wireless sensor networks. J. Xidian Univ., 37: 1125-1131.

Zhu, Q., C. Fung, R. Boutaba and T. Basar, 2012. GUIDEX: A game-theoretic incentive-based mechanism for intrusion detection networks. IEEE J. Sel. Areas Commun., 30: 2220-2230.