A Comprehensive Survey on Security Enhancement in Mobile Adhoc Networks using Game Theory Approaches

R.Sujitha
PG Student
Department of IT
National Engineering College

M.Kaliappan
Assistant Professor (SG)
Department of IT
National Engineering College

P.Subbulakshmi
Assistant Professor
Department of IT
National Engineering College

ABSTRACT
Enhancing security in Mobile Adhoc Network is a challenging issue. Mobile adhoc networks (MANET) designed to operate in more impetuous and swiftly changing environment. Enhancing MANET security is entirely different from the conventional methods of establishing security. There are many approaches in enhancing security in MANET.This paper discuss some techniques for belief evaluation of mobile nodes in MANET.In addition, this paper discusses about leader election scheme for mobile nodes.

Index Terms
Game Theory, Mobile Adhoc Network, Payoff, Reputation.

Keywords
Bayesian Game, Cooperative Game, Dynamic Bayesian Game, Mechanism Design Theory.

1. INTRODUCTION
In an adhoc network, Collaboration between the nodes is the considerable issue. mobile nodes communicate with each other using multihop wireless network Each node in the network also acts as a router, forwarding data packets for other nodes. Since all nodes are mobility in nature, they can move from one cluster to another cluster.Hence, nodes usually have no Predefined trust between each other.

To address the issue of enforcing cooperation among selfish nodes and to discriminate malicious nodes from regular nodes, belief evaluation and payment based schemes are used. Payoffs are numbers which represent the motivation of players. Ensuring security is inefficient in terms of resource consumption. To overcome this problem, a common approach is to divide the MANET into a set of 1-hop clusters where each node belongs to atleast one cluster. The nodes in each cluster elect a leader node to serve as the IDS for entire cluster.

2. LITERATURE SURVEY
Security in MANET is a great Challenge for several applications. Game theory plays significant role to provide security in MANET. The ability to model individual, independent decision makers whose actions potentially affect all other decision makers' renders game theory particularly attractive to analyze the performance of ad hoc networks.

G.Theodorakopoulos and John S. Baras [6] designed malicious users in Unstructured Networks; They used game theory to examine the effect of Malicious Users. All users are modeled as payoff-maximizing strategic agents. Here, allowed the Bad users to have all information about the past (their own moves, as well as everybody else's moves since the first round). On the other hand, the Good users follow a fictitious play process, so, at each round they are choosing the action that maximizes their payoff given the estimates they have for each of their neighbors' strategies.

Feng Li and Jie Wu [5] used Certainty Oriented Reputation System to update the Belief. they used an uncertainty metric to directly reflect a node's confidence in the sufficiency of its past experience. They introduced the concept of uncertainty, expand the subjective logic and design a certainty oriented reputation system to rationally evaluate trust Uncertainty increases transaction cost and decreases acceptance of communication and cooperation. Their objective is to reduce the trustor's perceived uncertainty so that transaction cost is lowered and a long-term exchange relationship is sustained.

See-Kee Ng, Winston K.G. Seah [4] suggested Game-Theoretic Model for Collaborative Protocols in Selfish, Tariff-Free, Multihop Wireless Network to apply game theory to achieve collusive networking behavior. The model applied the theory of imperfect private monitoring in game theory, and through the adaptation of Aoyagi's game of imperfect private monitoring and communication transforms the problem into a wireless multihop game model. They also focused on the problem of selfish behavior in MANETs.

S. Buchegger and Jean-Yves Le Boudec [13] discussed about reputation system and trust opinions for nodes. In their approach, everyone maintains a reputation rating and a trust rating about everyone else that they care about. Trust ratings are updated based on the compatibility of second-hand reputation information with prior reputation ratings. Also, standard Bayesian method is used to give weight of each observation. Reputation rating is used to reveal the truth about other nodes.

Pietro Michiardi and Refik Molva [14] described in their paper about Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks. In this Paper, the reputation is calculated based on various types of information on each entity's rate of collaboration. Behind this, only a cooperative behavior allows an entity to change its reputation value from negative to positive: disadvantaged nodes that are inherently selfish due to their precarious energy conditions shouldn't be excluded from the network using the same basis as for malicious nodes. This is done with an accurate evaluation of the reputation value.

3. SECURITY ENHANCEMENT USING GAME THEORY APPROACHES

3.1 Dynamic Bayesian Game
Feng Li and Jie Wu [1] used Dynamic Bayesian Game, Where wrestle between the regular and malicious nodes is resolved. Two strategies behind this game are pure strategy and mixed strategy. In Pure strategy, player does not change its type in

any situation. In Mixed Strategy, Player may change its type based on the probability.

Belief Evaluation

In this game, node updates its belief based on Certainty-Oriented Reputation System (CORS).In the CORS, node uses Bayesian inference, to estimate its neighbor's type based on its accumulated observation. Reputation is the opinion of one entity towards another based on past experiences and is represented as: belief and disbelief. To evaluate belief and disbelief, First-hand information and second-hand information gathering is used.

The reputation of a node computed from first-hand information is the reputation based on one's own experience. It is calculated directly from node's observation. It also propagates this information so that other nodes can use it as second-hand information. Each node has prior Beta (1, 1). When a new observation is made, if it is a successful forwarding, then α is updated. Otherwise, β is updated. The prior is then updated as Beta (α,β)). belief(b),disbelief(d) and uncertainty(u) is calculated from this observation.

Second-hand information is the information that a node gets from the first-hand information published by other nodes. It is a kind of trust transitivity. Node say A, first gathers other nodes' first-hand observations (in α,β) towards a particular node, say B, which it required to form belief. node A then converts the information (in α,β) into an opinion (in b; d; u) and discounts it by node A' s opinion towards the node reporting the observation. Author calls this the recommendation calculation. After gathering all the recommendations, node A will synthesize them and integrate the second-hand information with the first-hand observation and make a final anticipation and decision.

Calculating Payoff

Payoff is given to all nodes for participating in communication, especially for forwarding. Bayesian game uses Payoff matrix to calculate Payoff for choosing the action. Each node's aim is to maximize their payoff. So, maximum value of expected payoff is selected and corresponding action is chosen to communicate. According to this game, this technique motivates the selfish users to cooperate.

The tabular form for calculating Payoff is as follow.

Table 1:calculating Payoff

R / **S**	**Action1**	**Action2**	**Action3**
Action1	Payoff 11	Payoff 12	Payoff 13
Action2	Payoff 21	Payoff 22	Payoff 23
Action3	Payoff 31	Payoff 32	Payoff 33

Where S is Sender and R is Receiver. Expected Payoff (Action n) =θ*Payoff, if it is Pure strategy.

Expected Payoff (Action n) =Φ* θ*Payoff, if it is Mixed Strategy. Where n=1, 2, 3...

3.2 Belief Based Packet Forwarding

Zhu ji [2] suggested Two Player Belief based Packet Forwarding and multiplayer based packet forwarding approach. Belief Evaluation and payoff are calculated for former and latter.

3.2.1 Two player Belief Based Packet Forwarding

Two strategies are defined. One is trigger cooperation strategy, in which the player forward packets at current stage, and at the next stage, the player will continue to forward packets only if it observes the other player's forwarding signal. Another is, Continuation Strategies, Where the player always drops packets regardless of its observation history. Since both of the two strategies also determines the player's following action at every private history, the strategy path and expected future payoffs caused by any pair of the two strategies are fully specified by the author.

Belief Evaluation

Node initializes its belief of the other node as and chooses the forwarding action in period1.Then update its Belief based on the private history

The Player's new belief when takes action and receives signal can be defined using Baye's rule. First Belief is formed and then Belief is updated. If the updated belief is greater than belief of other node, then node prefers trigger cooperation strategy. Otherwise it chooses continuation strategy.

Calculating Payoff

In this scheme, Payoff is calculated using Bellman equation. payoff chooses action for Continuation strategy as pair such as FF, FD, DF, and DD where F, D represents Forwarding and dropping actions respectively. Bellman equation breaks a dynamic optimization problem into simpler subproblems, representing payoff of a dynamic programming problem at a certain point .Here, payoff value of FF should be greater than DF, so that it is possible to enforce cooperative behavior among selfish users.

3.2.2 Multinode Multihop Packet Forwarding

In the Multiplayer packet forwarding game, interaction among selfish nodes is modeled and optimal belief evaluation framework is developed based on the two-player belief system. As relay nodes play significant role in forwarding, source node select only some relay nodes based on the belief value. Belief evaluation is done as follow.

Belief Evaluation

For evaluating belief, Belief-based multihop packet forwarding strategy (BMPF) is modeled. According to this strategy, the sender and relay nodes act as follows.

***1. Game Partition and belief initialization*:**
Partition the original game into N subgames.then, each node initializes its belief of other nodes and forwards with probability.

2. Route Participation: The selected relay node on each route participates in the routing if and only if its belief is greater than belief of other node.

3. Route Selection: The sender selects the route with the largest belief from the route candidates.

4. Packet forwarding: The sender updates its belief of each relay node's continuation strategy using Baye's rule.

According to author, during the route participation stage, only the nodes with mutual beliefs that are greater than cooperation threshold can form a forwarding multihop route. This packet forwarding and belief evaluation specified by BMPF Strategy lead to a sequential equilibrium.

Payoff

The total payoff of each node can be improved if it participates in multihop packet forwarding following the BMPF Strategy. As each node is selfish and trying to maximize its own payoff, all nodes are inclined to follow the above strategy for achieving optimal payoff.

3.3 Mechanism Design Theory

Noman Mohammed et.al [3] suggested mechanism design based game theory to balance energy for all nodes and to act as IDS,a leader is elected from each cluster and selected leader performs some services. Leader Election is done based on cost of analysis and Reputation system.

Cost of Analysis Function

According to Noman Mohammed et.al, the energy level of each node is kept as private and sensitive information and should not be disclosed publicly, Since disclosure of information can be used maliciously for attacking the node with the least resources level.

To solve these problems, they designed the cost of analysis function with the following two properties: Fairness and Privacy. The former is to allow nodes with initially less resources to contribute and serve as leaders in order to increase their reputation. On the other hand, the latter is needed to avoid the malicious use of the resources level, which is considered as the most sensitive information.

The cost of analysis is designed based on the reputation value, the expected number of time slots that a node wants to stay alive in a cluster, and energy level. The cost of analysis is calculated through dividing the percentage of sampling by the power factor. The cost of

analysis is inversely proportional to the power factor. Using cost of analysis, energy level of each node is determined.

Reputation System

Reputation system model acts as belief evaluation of nodes in this leader election process. Objective is to: 1) motivate nodes to behave normally and 2) punish the misbehaving nodes. Misbehaving nodes are punished bydecreasing their reputation, and consequently, are excluded from the cluster services if the reputation is less than a predefined threshold. In this game, each node has the following components:

1. Monitor or watchdog: It is used to monior the behavior of the elected leader

Information exchange: It includes two types of information sharing:

a. The exchange of reputation with other nodes in other clusters (i.e., for services purposes).

b.To reduce the false positive rate, the checkers will exchange information about the behavior of the leader to make decision about the leader's behavior.

***2. Reputation system*:** The node that has the highest reputation can be considered as the most trusted node and is given priority in the cluster's services.

3. Threshold check: It has two main purposes: - 1. To verify whether nodes' reputation is greater than a predefined threshold. If the result is true then nodes' services are offered according to nodes' reputation.

2. To verify whether a leader's behavior exceeds a predefined misbehaving threshold. According to the result, the punishment system is called.

4. Service system: To motivate the nodes to participate in every election round, the amount of detection service provided to each node is used which is based on reputation value. Each elected leader has a budget for sampling, and thus, only limited services can be offered.

Finally, Reputation with highest value is elected as leader and this Reputation value motivates the selfish users to participate in cooperation.

4. Performance Analysis

Various mechanisms has been explained in previous sections. Table 2 describes some of the security parameters with limitations of above mechanisms.

Table 2:Comparison Table

Game Type / **Security Parameters**	**Dynamic Bayesian signaling Game**	**Belief Based Packet forward**	**Mechanism Design Theory**
Sensitive Information	Node's Type (regular or Malicious)	Observation about other nodes	Energy level
Attack	Dropping attack, Jamming Attack, Sybil attack	Malicious cheating behavior, Dropping attack	Replay attack, Malicious use of resource level
Demerits	Unsecured for multi attackers.	Belief under imperfect observ-ation	Increased leaders for increasing cluster size
Merits	Reduce Malicious node's utility	Enforce Cooperation under noisy and imperfect observ - ation	Motivate selfish nodes and balance resource usage

5. Conclusion

Adhoc network security has become significant for network security over the past couple of years. MANET Security requires countermeasures for misbehaving nodes. In this Paper, we describe a brief survey about the problems of misbehaving nodes and the solutions using game theoretical approach and also analyzed the merits and limitations of each technique. We also studied importance to enforce node's cooperation.

6. REFERNCES

[1] Feng Li & Jie Wu ,"Attack and Flee:Game Theory Based Analysis on Interactions Among Nodes in MANETs", IEEE Transactions on Systems,MAN and Cybernetics,June 2010,Volume 40,No 3.

[2] Zhu ji,Wei Yu and K.J Ray Liu,"A Belief Evaluation Framework in Autonomous MANETs under Noisy and Imperfect Observation:Vulnerability Analysis and Cooperation Enforcement", IEEE Transactions on Mobile Computing,September 2010,Volume 9,No 9.

[3] Noman Mohammed, Hadi Otrok, Lingyu Wang," Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET", IEEE Transactions on Dependable and Secure Computing.Vol. 8, No 1, Jan 2011.

[4] S. Ng and W. Seah, "Game-theoretic model for collaborative protocols in selfish, tariff-free, multihop wireless networks," in Proc. IEEE INFOCOM, 2008.

[5] F. LI AND J. WU, "Mobility reduces uncertainty in MANETs," in Proc. IEEE INFOCOM, 2007.

[6] G. Theodorakopoulos and J. Baras, "Malicious users in unstructured networks," in Proc. IEEE INFOCOM, 2007, pp. 884–891.

[7] P. Nuggehalli, M. Sarkar, K. Kulkarni, and R. Rao, "A game-theoretic analysis of QoS in wireless MAC," in Proc. IEEE INFOCOM, 2008

[8] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in Proc. ACM GameNets, 2006

[9] M. Felegyhazi, J. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," IEEE Trans. Mobile Comput., vol. 5, no. 5, pp. 463–476, May 2006.

[10] P. Liu, W. Zang, and M. Yu, "Incentive-based modeling and inference of attacker intent, objectives and strategies," ACM Trans. Inf. Syst. Secur.,vol. 8, no. 1, Feb. 2005.

[11] A. Blanc, Y. Liu, and A. Vahdat, "Designing incentives for peer-to-peer routing," in Proc. IEEE INFOCOM, 2005

[12] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Stanford Univ. Press, Stanford, CA, Tech. 2003.

[13] S. Buchegger and J. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in Proc. 2nd Workshop Econ. Peer-to-Peer Syst., 2004.

[14] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc.Commun. Multimedia Secur., 2002.

[15] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Stanford Univ. Press, Stanford, CA, Tech. 2003