IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 2, Ver.1 (Mar - Apr.2015), PP 101-112
www.iosrjournals.org

Protection Augmentation in Mobile Ad Hoc Networks Using Game Theory

Saravanan T, Mr.P.Rajkumar, M.E.,
M.E in Communication Systems (ECE), Final Year Varuvan Vadivelan Institute of Technology, Dharmapuri, India
Asst Prof, ECE Dept, Varuvan Vadivelan Institute of Technology, Dharmapuri, India

Abstract: *Game theory can provide a useful tool to study the security problem in mobile ad hoc networks (MANETs). Most of existing works on applying game theories to security only consider two players in the security game model: an attacker and a defender. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available. In this paper, using recent advances in mean field game theory, we propose a novel game theoretic approach with multiple players for security in MANETs. The mean field game theory provides a powerful mathematical tool for problems with a large number of players. The proposed scheme can enable an individual node in MANETs to make strategic security defence decisions without centralized administration. In addition, since security defence mechanisms consume precious system resources (e.g., energy), the proposed scheme considers not only the security requirement of MANETs but also the system resources. Moreover, each node in the proposed scheme only needs to know its own state information and the aggregate effect of the other nodes in the MANET. Therefore, the proposed scheme is a fully distributed scheme. Simulation results are presented to illustrate the effectiveness of the proposed scheme.*

Index Terms: *Mean field game, security, mobile ad hoc network (MANET).*

I. Introduction

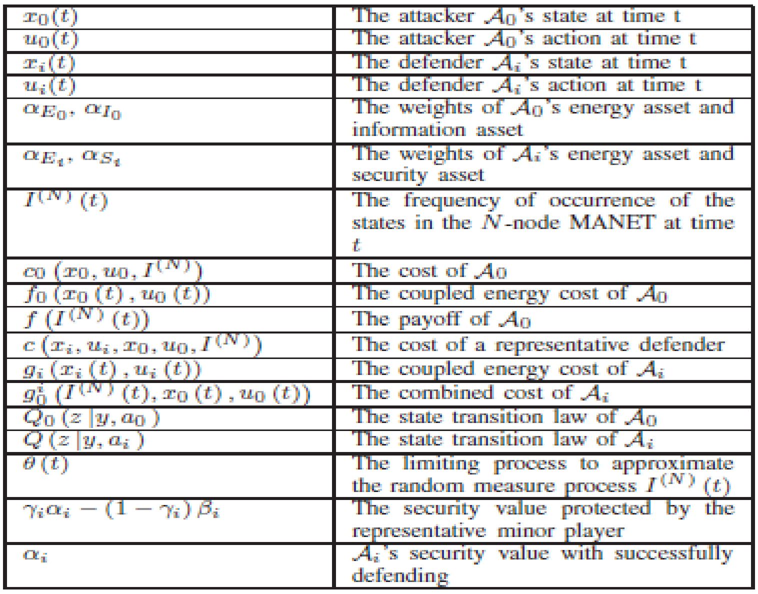
AS wireless networking becomes almost omnipresent, security has become one of the key issues in the research field of mobile ad hoc networks (MANETs). In a MANET, mobile nodes can autonomously organize and communicate with each other over bandwidth-constrained wireless links. A wireless mobile node can function both as a network router for routing packets from the other nodes and as a network host for transmitting and receiving data. The topology of the MANET changes dynamically and unpredictably because of nodes mobility. Many distributed algorithms have been studied to determine the networking organization, routing, and link scheduling. On the other hand, the unique characteristics of MANETs present some new challenges to security design due to the lack of any central authority and shared wireless medium [1], [2]. There are various security threats that exist in MANETs, such as denial of service, black hole, resource consumption, location disclosure, wormhole, host impersonation, information disclosure, and interference [3], [4].

A number of researchers have investigated the security issues in MANETs. Basically, there are two complementary classes of approaches to secure a MANET: prevention-based approaches, such as authentication, and detection-based approaches, such as intrusion detection systems (IDSs) [3], [5], [6]. Zhang and Lee in [7] not only presented the basic requirements for an IDS that works in the MANETs environment, but also proposed a general intrusion detection and response mechanism for MANETs. In their proposed scheme, each IDS agent is involved in the intrusion detection and response tasks independently. Authentication is an important type of responses initiated by an IDS. After an authentication process, only authenticated users can continue using the network resources and compromised users will be excluded [8].

Recently, game theoretic approaches have been proposed to improve network security [9], [10]. Game theory is a useful tool to provide a mathematical framework for modeling and analyzing decision problems, since it can address problems where multiple players with contradictory goals or incentives compete with each other. In game theory, one player's outcome depends not only on his/her decisions, but also on those of others' decisions. Similarly, the success of a security scheme in MANETs depends not only on the actual defense strategies, but also on the actions taken by the attackers. Bedi et al. modeled the interaction between the attacker and the defender as a static game in two attack scenarios: one attacker for DoS and multiple attackers for DDoS [11]. The concept of multi-stage dynamic non-cooperative game with incomplete information was presented in [12], where an individual node with IDS can detect the attack with a probability depending on its belief updated according to its received messages. In [13], the authors integrated the ad hoc on-demand distance vector (AODV) routing protocol for MANETs with the game theoretic approach. The benefit is that each node can transfer its packets through the route with less energy consumption of host-IDS and less probability of attack with the optimal decision. A framework that combines the N-intertwined epidemic model with non-cooperative game model was proposed in [14], where the authors showed that the network's quality largely depends on the underlying topology. Researchers also tried to build an IDS based on a cooperative scheme to detect intrusions in MANETs [15]. The authors of [16] considered a Bayesian game to study the interaction between the legitimate nodes and the malicious nodes. The malicious nodes try to deceive the legitimate nodes by cooperating with them to get better payoffs, and the legitimate nodes choose a probability to cooperate with the malicious nodes and decide whether or not to report misbehaviors based on their consistently updated beliefs.

Although some excellent research has been done on addressing the security issues in MANETs using game theoretic approaches, most of the existing work only considered a security game model with two players in the security game model: an attacker and a defender. For the problem scenarios with multiple attackers versus multiple defenders, the security game is usually modeled as a two-player game in which the whole of the defenders is treated as one player, as is the whole of attackers [10]. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available. Consequently, each individual node in a MANET should be treated separately in the security game model. In this paper, using recent advances in mean field game theory [17], we propose a novel game theoretic approach for security in MANETs. The mean field game theory provides a powerful mathematical tool for problems with a large number of players. It has been successfully used by economists, socialists, and engineers in different areas, among others [18]. In communication networks, several researchers have tried to use mean field approximation method and mean field game theories to solve the energy efficiency [19] and medium access control [20] problems. To the best of our knowledge,using mean field game theoretic approach for security in MANETs has not been considered in the existing works.

Table I Main Notations



$x_0(t)$	The attacker $\mathcal{A}_0$'s state at time t
$u_0(t)$	The attacker $\mathcal{A}_0$'s action at time t
$x_i(t)$	The defender $\mathcal{A}_i$'s state at time t
$u_i(t)$	The defender $\mathcal{A}_i$'s action at time t
$\alpha_{E_0}, \alpha_{I_0}$	The weights of $\mathcal{A}_0$'s energy asset and information asset
$\alpha_{E_i}, \alpha_{S_i}$	The weights of $\mathcal{A}_i$'s energy asset and security asset
$I^{(N)}(t)$	The frequency of occurrence of the states in the N-node MANET at time t
$c_0\left(x_0, u_0, I^{(N)}\right)$	The cost of $\mathcal{A}_0$
$f_0\left(x_0(t), u_0(t)\right)$	The coupled energy cost of $\mathcal{A}_0$
$f\left(I^{(N)}(t)\right)$	The payoff of $\mathcal{A}_0$
$c\left(x_i, u_i, x_0, u_0, I^{(N)}\right)$	The cost of a representative defender
$g_i\left(x_i(t), u_i(t)\right)$	The coupled energy cost of $\mathcal{A}_i$
$g_0^i\left(I^{(N)}(t), x_0(t), u_0(t)\right)$	The combined cost of $\mathcal{A}_i$
$Q_0\left(z \mid y, a_0\right)$	The state transition law of $\mathcal{A}_0$
$Q\left(z \mid y, a_i\right)$	The state transition law of $\mathcal{A}_i$
$\theta(t)$	The limiting process to approximate the random measure process $I^{(N)}(t)$
$\gamma_i\alpha_i - (1-\gamma_i)\beta_i$	The security value protected by the representative minor player
α_i	$\mathcal{A}_i$'s security value with successfully defending

The contributions of this work are as follows.

- We propose a dynamic mean field game theoretic approach to enable an individual node in MANETs to make strategic security defence decisions without centralized administration.
- Since security defence mechanisms in a wireless mobile node consume precious system resources (e.g., energy), the proposed scheme considers not only the security requirement of MANETs but also the system resources.
- In the proposed mean field game theoretic approach, each node only needs to know its own state information and the aggregate effect of the other nodes in the MANET. Therefore, the proposed scheme is a fully distributed scheme.

Simulations results are presented to show the effectiveness of the proposed scheme. The main notations used in this paper are summarized in Table I. The rest of this paper is organized as follows. We describe the system model and the mean field game formulation in Section II. The approximation approach of the mean field process and the solution to the mean field system are introduced in Section III. We also discuss the assumption of the ϕ function and the formulation of the cost in this section. In Section IV, we give an example to show how to derive the stochastic distributed optimal defending strategy in MANETs. The simulation results are discussed in Section V. Finally, we conclude this study in Section VI with future work.

II. System Description And Mean Field Game Formulation

In this section, a system that contains an N-node MANET and an attacker is presented. Then the security problem of this system is formulated as an N + 1 mean field game.

A. System Model

Fig. 1 illustrates an N-node MANET and an attacker that can attack the MANET dynamically. The legitimate nodes are independent because there is no centralized administration in the MANET. When the attacker has successfully attacked the MANET, some rewards (e.g., secret information) can be acquired by the attacker from the MANET. If the attacker failed because of the target node launching the defence action, some rewards (e.g., attack information) will be given to the target MANET node for its successful defence. Furthermore, the attacker and the defenders all need to pay the cost (e.g., energy consumption) for their individual actions. We model this system as an N +1 mean field game model as follows. We consider the defending MANET nodes as the N minor players. Meanwhile, the attacker, which tries to attack the MANET, is considered as a major player A0. Fig. 2 illustrates the interactions between the major player and the minor players in the MANET. We define the attacker's state space and action space as S0 = {1, ・ ・ ・ ,K0} and

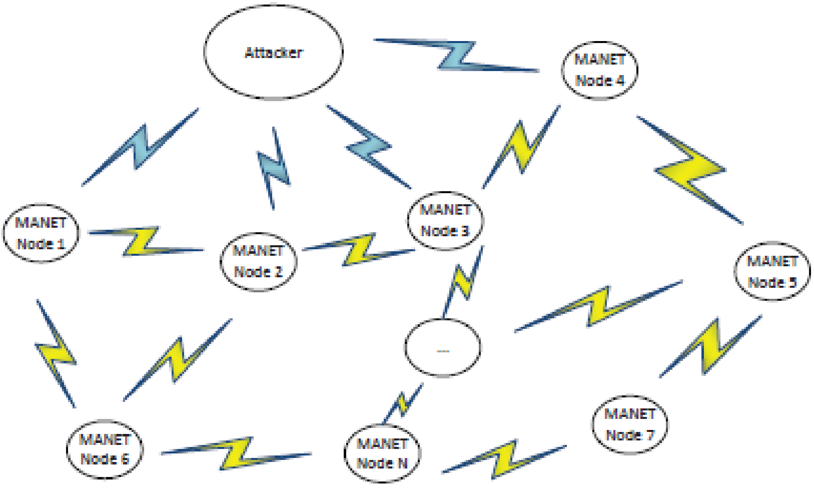


Fig. 1. A N-node MANET with an attacker.

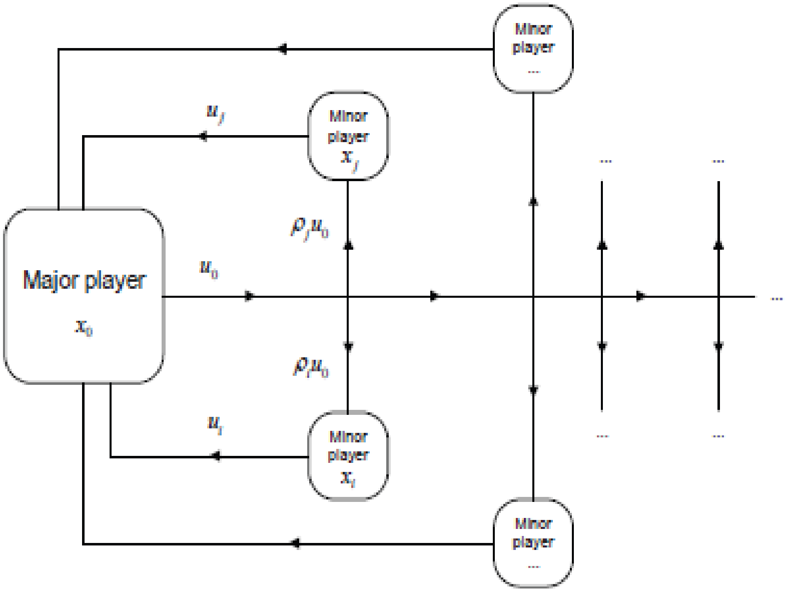


Fig. 2. The mean field game model of a MANET with mixed players. (x0: state of major player; xi,xj : states of minor players i and j; u0: action of major player; ui and uj : actions ofminor player i and j; ρi and ρj : weights of major player's action.)

A0 = {1, ・ ・ ・ , L0}, respectively. Meanwhile, the defenders' state space and action space are S = {1, ・ ・ ・ ,K} and A = {1, ・ ・ ・ , L}, respectively. At time t ∈ Z+ = {0, 1, 2, ・ ・ ・ }, we define that the attacker A0's state is x0(t) and its action is u0 (t). Similarly, the state and the action of a representative legitimate node Ai, i ∈ (1, ・ ・ ・ ,N) are denoted as xi (t) and ui (t), respectively.

B. States, Transition Laws, and Cost Functions

The major player's state is defined as a combination of energy and information assets, which can be denoted by αE0E0 + αI0I0 [21], in which αE0 and αI0 represent the weights of energy and the information assets, respectively. Meanwhile, the minor players' state is defined as a combination of energy and security assets, which is denoted by αEiEi + αSiSi, in which αEi and αSi represent the weights of the energy and the security assets, respectively. The average state of all the minor players is denoted by I(N) (t) and

$$\mathrm{I}^{(\mathrm{N})}(\mathrm{t}) = \left(\mathrm{I}_1^{(\mathrm{N})}(\mathrm{t}), \ldots, \mathrm{I}_{\mathrm{K}}^{(\mathrm{N})}(\mathrm{t})\right), (\mathrm{t} \geq 0), \qquad (1)$$

Where $\mathrm{I}_{\mathrm{K}}^{(\mathrm{N})}$ (t) = $\frac{1}{\mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{N}}$ 1 (xi$_{(\mathrm{t})=\mathrm{K}}$).$\mathrm{I}^{(\mathrm{N})}$ (t) represents the frequency of occurrence of the states in S in the mean field at time t.

Additionally, Q0 (z |y, a0) and Q(z |y, ai) represent the state transition laws of the major player and representative minor player, respectively. The state transition of the major player is specified by

Q0 (z|y, a0) = P (x0 (t + 1) = z|x0 (t) = y, u0 (t) = a0) , (2)

where y, z ∈ S0 and a0 ∈ A0. For minor player Ai, the state transition law is determined by

Q(z|y, a) = P (xi (t + 1) = z|xi (t) = y, ui (t) = a) , (3)
where y, z ∈ S, and a ∈ A.

The instantaneous costs of the major player and the representative minor player can be denoted by c0 x0 (t) , u0 (t), $\mathrm{I}^{(\mathrm{N})}$ (t) and ci xi (t) , ui (t), x0 (t) , $\mathrm{I}^{(\mathrm{N})}$ (t), respectively.

However, when we consider the game process, ci xi (t) , ui (t), u0 (t) , $\mathrm{I}^{(\mathrm{N})}$ (t) should be considered. Because it is believed that the impact of the major player to the representative minor player's instantaneous cost is not directly from the state x0 (t), but directly from the action u0 (t). In other words, for the representative minor player, at time t, the result of the game is not only determined by its action under certain state, but also depending on which action the major player takes under some state. We define the instantaneous cost of the major player as follows:

c0 x0 (t) , u0 (t), $\mathrm{I}^{(\mathrm{N})}$ (t)

= f0 (x0 (t) , u0 (t)) – f ($\mathrm{I}^{(\mathrm{N})}$ (t)), (4)

where f0 (x0 (t) , u0 (t)) denotes the coupled energy cost when the major player adopts different actions under various states. For example, when one state is "full energy" and the major player could choose the action to strongly attack the whole network. As a result, the energy cost is much higher than the one when the state is "poor energy" and the major player
does not attack. f($\mathrm{I}^{(\mathrm{N})}$ (t)) denotes the payoff of the major player, which comes from the attacking. f($\mathrm{I}^{(\mathrm{N})}$ (t)) should also represent the average reflection of the whole mean field to the major player's attack. Meanwhile, we also define the cost of a representative minor player i as follows:

ci (xi (t) , ui (t), x0 (t) , u0 (t) , I(N) (t))
=gi (xi (t), ui (t)) + gi0 (I(N) (t), x0 (t) , u0 (t)), (5)

In the equation above, gi (xi (t) , ui (t)) denotes the coupled cost when the representative minor player adopts different actions under one state. gi0(I(N) (t), x0 (t) , u0 (t)) represents the combined cost from the influence of the major player's state, action, and the reflection of the whole mean filed.

The interactions between the major player (as an attacker) and a representative minor player (as a defender) are modelled as a non-cooperative non-zero-sum game. We define that the minor player Ai' security value is worth of wi, where wi > 0. wi can be the value of the protected assets in practice and –wi represents a loss of security. In this model, we also assume that the loss wi of the minor player Ai is equal to the gain of the major player A0 from Ai. However, the A0 could gain the i=1 ,wi from different minor players at the same time. The
game model of the ad hoc network with a major player and several minor players is shown as Fig. 2.

III. Simulation Results And Discussions

We consider the following simulation scenarios: A MANET consists of N nodes, each of which is equipped with IDS sensors. The number of nodes in the MANET will be changed
in the simulations (such as N = 20, 40, 60, 80, 100). There is a malicious node that wants to attack this MANET. The malicious node is considered as the major player. The N nodes in the MANET are the minor players and they can detect the intrusion with the help of IDS sensors operating independently.

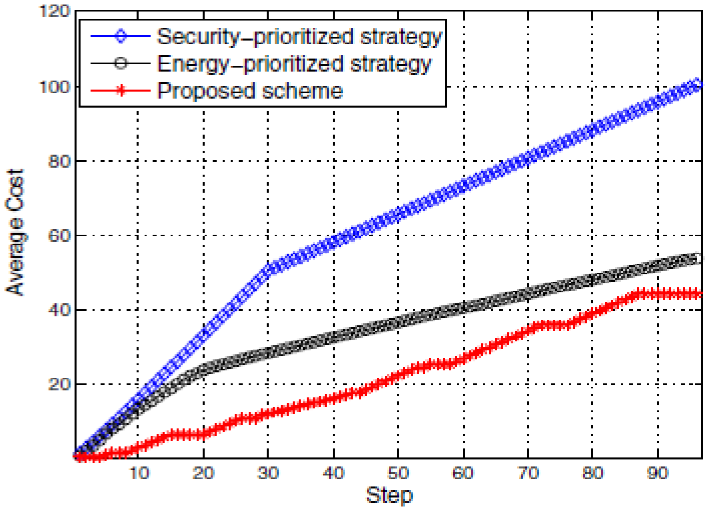


Fig. 4. Average cost comparison among the representative minor player in different schemes (under the dynamical attack).

We compare the performance of a representative node, which adopts the optimal strategy along with the performance of adopting other two strategies. The average lifetime and the compromising probability of the MANET are also compared. We also consider the situation of the nodes in the MANET with sufficient energy. The decrease of compromising probability and the improvement of lifetime using the optimal strategy are depicted. First of all, the major player in the system starts with a dynamic state x0 ∈ S0. It evolutes with its optimal updating rule and attacks the minor players randomly. The minor players' states start with safe and full energy and then they are updated with one of the two optimal updating rules, which are based on the influence of the major player. The minor players can detect the actions of the major player by the IDS sensors, which are equipped in each node.

A. Average Cost

Using the cost function defined in (24), we perform the simulation 200 times and calculate a representative minor player's the average cost of each step. We compare the average cost under different strategies, such as the security prioritized strategy, the energy-prioritized strategy, and the optimal strategy. In the energy-prioritized strategy, energy is the primary concern of the mobile nodes (e.g., in commercial MANETs) [23], while security is the primary concern in the security-prioritized strategy (e.g., in military MANETs) [24]. From Fig. 4, we can see that the proposed scheme has the lowest cost compared with the other two strategies. In other words, each minor player can greatly reduce energy consumption and loss of security information with the optimal strategy. When the major player attacks continuously, as illustrated in Fig. 5, the average cost when the minor player adopts the optimal strategy is also the lowest compared with the other two strategies.

B. Defence Actions According to Optimal Strategy

In the simulation, we study minor players' defence actions when the attacker launches continuous attack and dynamic attack, respectively. We choose a MANET with 20 nodes (N = 20) and capture nodes' actions in each step. All the MANET nodes use the optimal strategy derived in our scheme.

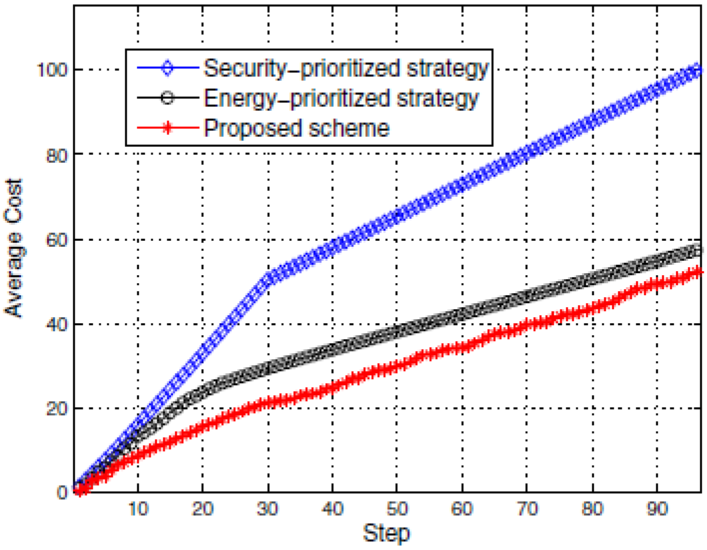


Fig. 5. Average cost comparison among the representative minor player in different schemes (under the continuous attack).

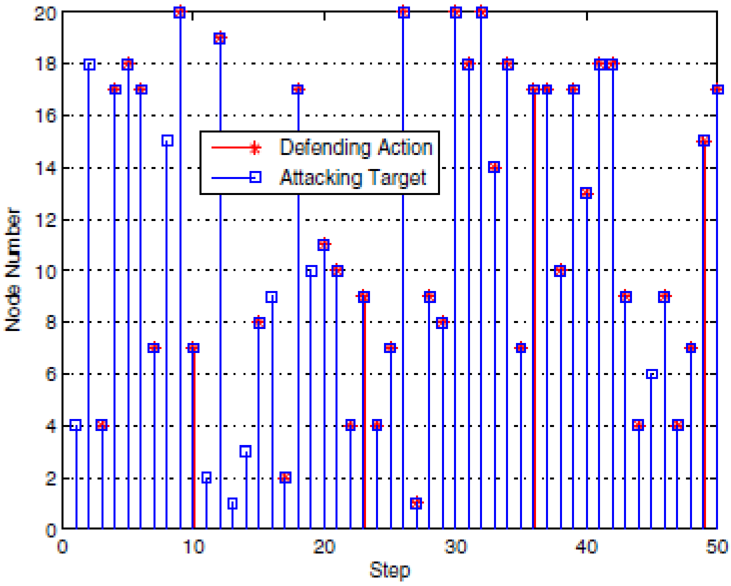


Fig. 6. Attacking target and defence action under major player's continuous attack).

In Fig. 6, the attacker launches continuous attack and it chooses attacking target dynamically. We records and observes the dynamic change of the target node's action with the proposed scheme in the first 50 steps. From the simulation result, we can see that the defender being attacked in each step does not always choose the defending action with the optimal strategy, because the decision making is according to whether or not the node's current state is proper to defend at this moment. In other words, the defending action may not always be the best choice for nodes in MANETs when we try to extend the average lifetime and reduce the compromising probability of MANETs. When the attacker launches dynamic attack, the dynamic change of the target node's actions in the first 50 steps is presented in Fig. 7. In this situation, the attacking target is also chosen dynamically in each step by the attacker. Compared with Fig. 6, there is no node being attacked in some steps, because the attacker does not attack continuously. The simulation result illustrates that even if the node is attacked

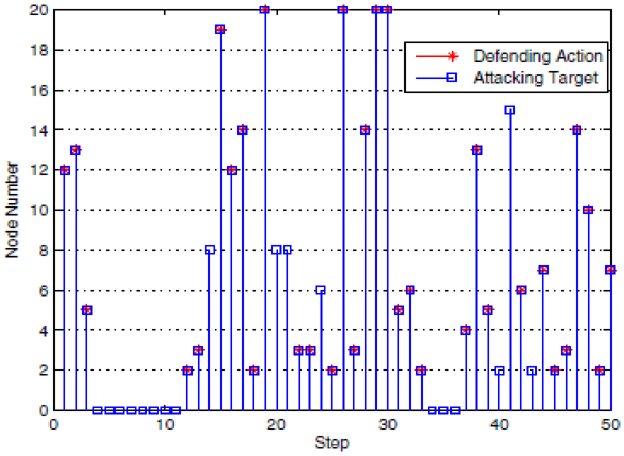


Fig. 7. Attacking target and defence action under major player's dynamical attack).

in one step, it does not choose the defending action all the time with the optimal strategy. In addition, in both Fig. 6 and Fig. 7, the nodes' actions are not defending when they are not the attacking targets according to the optimal strategy we got. Each node tries to control the energy consumption efficiently. So the lifetime of MANET can be extended.

B. Performance with Limited Energy

Network lifetime is one of the key performance metrics in the MANET. Here, we consider the network lifetime with two constraints. The first constraint is that if one node's energy consumption reaches 90%, the node cannot work well. When there are more than 70% nodes in the MANET that cannot work well, the MANET will be considered dead. The second constraint is that if the node's loss of security value reaches 80%, the node is compromised. The network is deemed compromised when there are more than 50% nodes in the MANET compromised. We assume that each node has the same initial value of the combination of energy and security. Fig. 8 illustrates the average lifetime of a MANET when the number of nodes increases from 20 to 100. With the increase of the number of available nodes, the lifetime of MANET will increase as well. Compared to the two other strategies, the proposed scheme has the best average lifetime due to the optimal strategy. The proposed method is more suitable for the MANET with larger number of nodes when they encounter dynamical attacks from the major player.

In these simulations, we also investigate the compromising probability of the MANET. When the number of compromised nodes is up to 15% of the total number of the nodes in the MANET, the whole MANET can be considered to be compromised. Fig. 9 illustrates a downward trend in compromising probabilities when the total number of nodes increases in the MANET. When the minor players adopt the optimal strategy, the MANET's compromising probability is always lower than the compromising probabilities when they adopt the two other strategies.

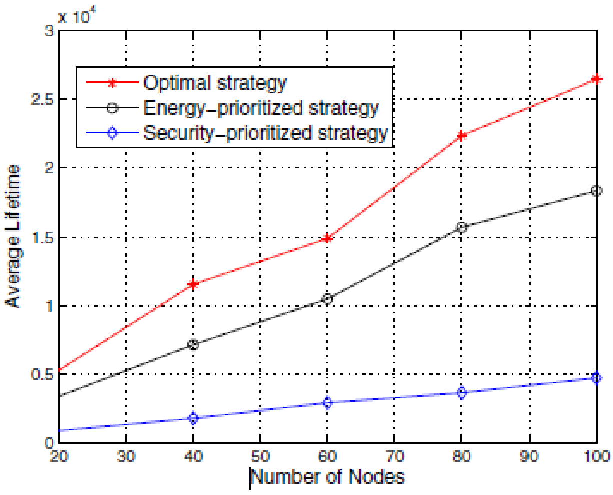


Fig. 8. Comparison of average lifetime with different numbers of nodes (limited energy).

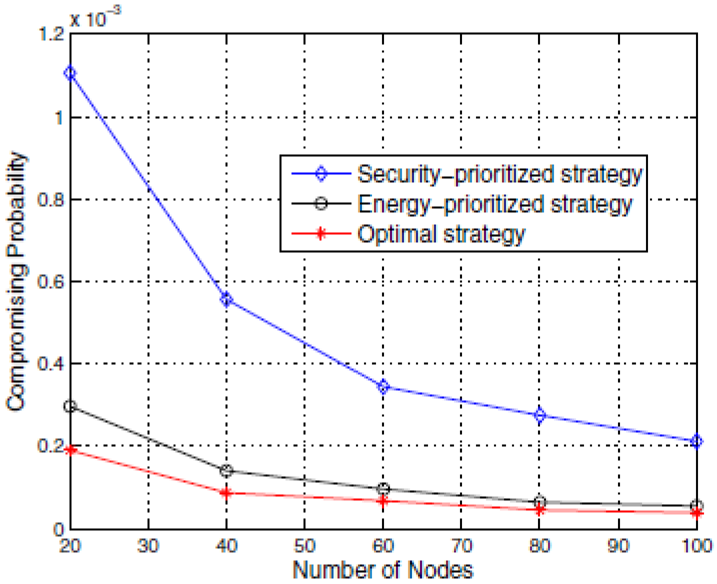


Fig. 9. Comparison of compromising probabilities with different numbers of nodes (limited energy).

D. Performance with Sufficient Energy

In some situations, the nodes in the MANET may be supplied with sufficient energy (e.g., vehicular ad hoc networks). So we only consider the security value loss as the criterion

to determine the lifetime. The results in Fig. 10 and Fig. 11 indicate that, although security-prioritized strategy can bring longer lifetime and lower compromising probability than the energy-prioritized strategy in this situation, our optimal strategy can provide the best performance for the MANET among these three strategies.

The effect of state transition probability (the first component in the state transition matrix of the representative minor player) on the network lifetime is shown in Fig. 12. We can see the better performance of the proposed scheme with different state transition probabilities. With the increase of the state transition probability, the network lifetime increases in all different strategies. This is because this state transition probability refers to the probability that the state remains in state “Safe” if it chooses action “Defending”. The higher the value of this state transition probability, the lower the probability that the node transits to state “Unsafe”, which means longer network lifetime.

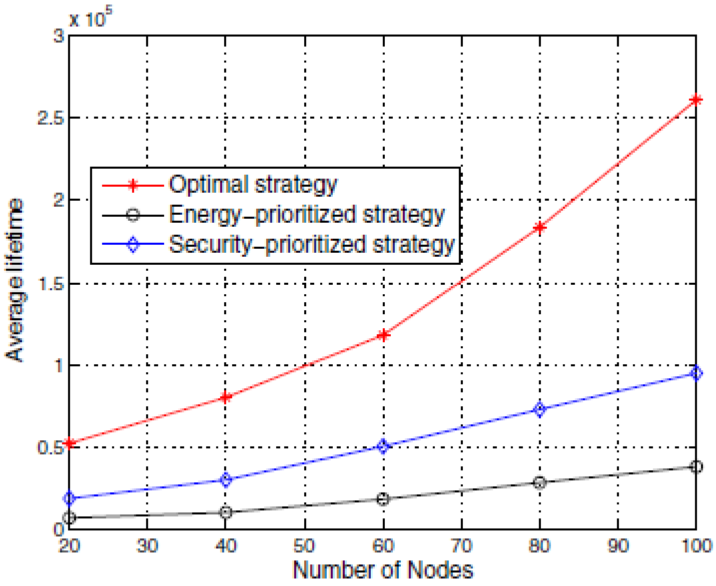


Fig. 10. Comparison of average lifetimes with different numbers of nodes (sufficient energy).

DOI: 10.9790/2834-1021101112

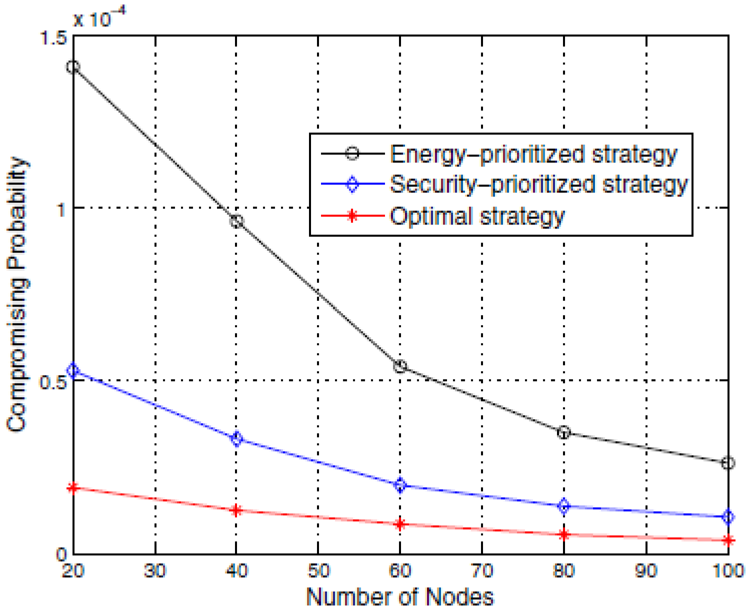


Fig. 11. Comparison of compromising probabilities with different numbers of nodes (sufficient energy).

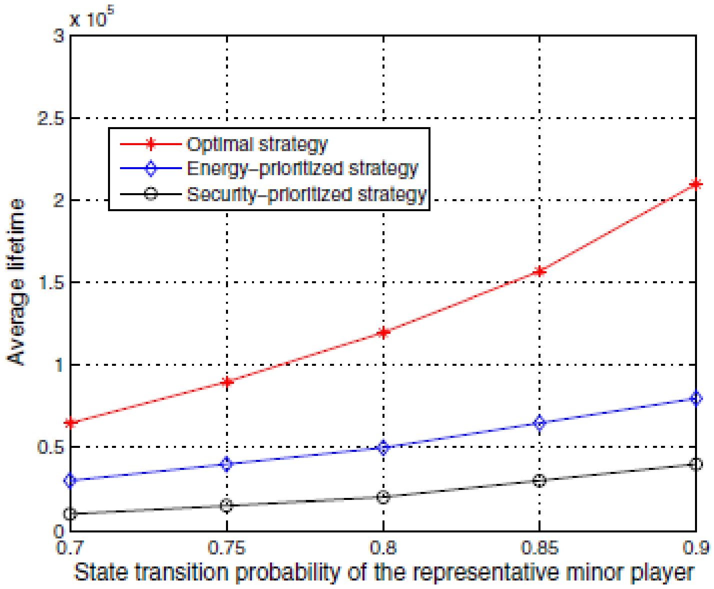


Fig. 12. Comparison of average lifetimes with different state transition probabilities of the representative minor player (sufficient energy).

IV. Protection Augmentation Using Game Theory

Game theoretic approaches have been proposed to improve network security. Game theory is a useful tool to provide a mathematical framework for modeling and analyzing decision problems, since it can address problems where multiple players with contradictory goals or incentives compete with each other. In game theory, one player's outcome depends not only on his/her decisions, but also on those of others' decisions. Similarly, the success of a security scheme in MANETs depends not only on the actual defense strategies, but also on the actions taken by the attackers. Bedi modeled the interaction between the attacker and the defender as a static game in two attack scenarios one attacker for DoS and multiple attackers for DDoS. The concept of multi-stage dynamic non-cooperative game with incomplete information was presented in where an individual node with IDS can detect the attack with a probability depending on its belief updated according to its received messages. In the authors integrated the ad hoc on-demand distance vector (AODV) routing protocol for MANETs with the game theoretic approach.

The benefit is that each node can transfer its packets through the route with less energy consumption of host-IDS and less probability of attack with the optimal decision. A framework that combines the N-intertwined epidemic model with non-cooperative game model was proposed in where the authors showed that the network's quality largely depends on the underlying topology. Researchers also tried to build an IDS based on a cooperative scheme to detect intrusions in MANETs. The authors of considered a excellent research has been done on addressing the security issues in MANETs using game theoretic approaches, most of the existing work only considered a security game model with two players in the security game model: an attacker and a defender. For the problem scenarios with multiple attackers versus multiple defenders, the security game is usually modeled as a two-player game in which the whole of the defenders is treated as one player, as is the whole of attackers. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available. Consequently, each individual node in a MANET should be treated separately in the security game model.

V. Our Newapproach For Security

The problem scenarios with multiple attackers versus multiple defenders, the security game is usually modeled as a two-player game in which the whole of the defenders is treated as one player, as is the whole of attackers. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available. Consequently, each individual node in a MANET should be treated separately in the security game model. Game philosophy can deliver a useful tool to study the safety problem in mobile ad hoc networks (MANETs). Most of obtainable works on smearing game theories to safety only consider two players in the security game typical an assailant and a protector. While this supposition may be valid for a network with centralized administration, it is not truthful in MANETs, where centralized administration is not available. In this paper, using recent improvements in mean field game theory, we propose a unique game hypothetical approach with multiple players for safety in MANETs. The mean field game theory provides a powerful mathematical tool for problems with a large number of players. The future scheme can enable an individual node in MANETs to make strategic security defense decisions without

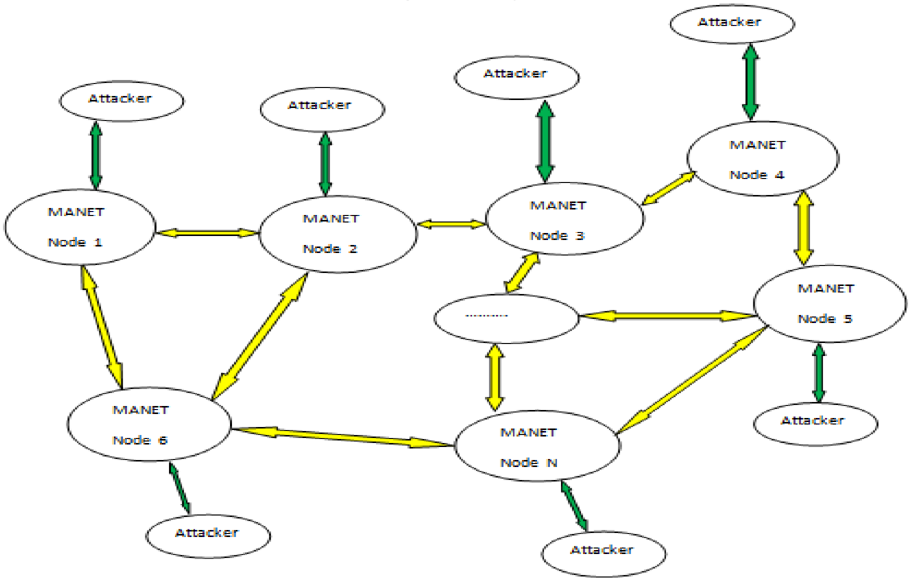


Fig. 13. System Architecture

Centralized administration. Furthermore, each node in the planned scheme only needs to know its own state information and the collective consequence of the other nodes in the MANET. In the proposed mean field game theoretic approach, each node only needs to know its own state information and the aggregate effect of the other nodes in the MANET. Therefore, the proposed scheme is a fully distributed. Consequently, the proposed scheme is a fully dispersed scheme. Simulation results are obtainable to illustrate the effectiveness of the proposed scheme with packet delivery ratio, Throughput, Delay and Energy.

A. Advantages

1. Dynamic Field Game approach
2. Energy with security
3. Evaluating packet delivery ratio, Throughput, Delay and Energy.

B.Modules

1. Network Setup
2. Energy with security
3. Gaming

1. Network Setup Model

The user can register and login with the owner permission to send data from one node to another node in the network. The data will travel through the topology because the number of nodes in the network is known as topology.

2. Energy with security

We propose a dynamic mean field game theoretic approach to enable an individual node in MANETs without centralized administration. This project considers not only the security requirement of MANETs but also the system resources. In the proposed mean field game theoretic approach, each node only needs to know its own state information and the aggregate effect of the other nodes in the MANET. Therefore, the proposed scheme is a fully distributed.

3. Gaming

Game theory is a useful tool to provide a mathematical framework for modeling and analyzing decision problems, since it can address problems where multiple players with contradictory goals or incentives compete with each other. In game theory, one player's outcome depends not only on his/her decisions, but also on those of others' decisions. Most of the existing work only considered a security game model with two players in the security game model an attacker and a defender. For the problem scenarios with multiple attackers versus multiple defenders, the security game is usually modeled as a two-player game in which the whole of the defenders is treated as one player, as is the whole of attackers.

While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available. Consequently, each individual node in a MANET should be treated separately in the security game model. The mean field game theory provides a powerful mathematical tool for problems with a large number of players. It has been successfully used by economists, socialists, and engineers in different areas, among others.

The concept of multi-stage dynamic non cooperative game with incomplete information was presented , where an individual node with IDS can detect the attack with a probability depending on its belief updated according to its received messages. the authors integrated the ad hoc on-demand distance vector (AODV) routing protocol for MANETs with the game theoretic approach. The benefit is that each node can transfer its packets through the route with less energy consumption of host-IDS and less probability of attack with the optimal decision. A framework that combines the N-intertwined epidemic model with non-cooperative game model was proposed, where the authors showed that the network's quality largely depends on the underlying topology. Researchers also tried to build an IDS based on a cooperative scheme to detect intrusions in MANETs.

The authors considered a Bayesian game to study the interaction between the legitimate nodes and the malicious nodes. The malicious nodes try to deceive the legitimate nodes by cooperating with them to get better payoffs, and the legitimate nodes choose a probability to cooperate with the malicious nodes and decide whether or not to report misbehaviors based on their consistently updated beliefs. Although some excellent research has been done on addressing the security issues in MANETs using game theoretic approaches, most of the existing work only considered a security game model with two players in the security game model an attacker and a defender. For the problem scenarios with multiple attackers versus multiple defenders, the security game is usually modeled as a two-player game in which the whole of the defenders is treated as one player, as is the whole of attackers. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available.

Consequently, each individual node in a MANET should be treated separately in the security game model. In this paper, using recent advances in mean field game theory , we propose a novel game theoretic approach for security in MANETs. The mean field game theory provides a powerful mathematical tool for problems with a large number of players. It has been successfully used by economists, socialists, and engineers in different areas, among others . In communication networks, several researchers have tried to use mean field approximation method and mean field game theories to solve the energy efficiency and medium access control problems. To the best of our knowledge, using mean field game theoretic approach for security in MANETs has not been considered in the existing works.

VI. Conclusions And Future Work

In this paper, we proposed a novel mean field game theoretic approach for security in MANETs to model the interactions among a malicious node and a large number of legitimate

MANET nodes. Unlike the existing works on security game modeling, the proposed scheme can enable an individual node in MANETs to make distributed security defence decisions. Both security requirement and system resources were considered in the proposed scheme. The simulation results demonstrated that, with the optimal strategy, the legitimate nodes can choose distributed actions intelligently to reduce their energy consumption and security value loss. The average lifetime of the MANET can be improved significantly and the compromising probability can be reduced as well. In our future work, we will extend our proposed scheme to the scenario of multiple attackers and multiple defenders. It is also interesting to consider MANETs with cognitive radios [25] in the proposed framework.

References

[1]. M. Carvalho, “Security in mobile ad hoc networks,” IEEE Security Privacy, vol. 6, no. 2, pp. 72–75, Mar. 2008.

[2]. F. R. Yu, H. Tang, S. Bu, and D. Zheng, “Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks,” EURASIP J. Wireless Commun. Netw., vol. 2013, no. 1, pp. 188–190, July 2013.

[3]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” IEEE Trans. Wireless Commun., vol. 11, pp. 38–47, Feb. 2004.

[4]. Q. Guan, F. R. Yu, S. Jiang, and V. Leung, “Joint topology control and authentication design in mobile ad hoc networks with cooperative communications,” IEEE Trans. Veh. Technol., vol. 61, no. 6, pp. 2674– 2685, July 2012.

[5]. J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, “Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks,” IEEE Trans. Wireless Commun., vol. 8, no. 2, pp. 806–815, Feb. 2009.

[6]. S. Bu, F. R. Yu, X. P. Liu, and H. Tang, “Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks,” IEEE Trans. Wireless Commun., vol. 10, no. 9, pp. 3064–3073, Sept. 2011.

[7]. Y. Zhang and W. Lee, “Intrusion detection in wireless ad hoc networks,” in Proc. 2000 ACM MOBICOM, pp. 275–283.

[8]. A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” IEEE Trans. Wireless Commun., vol. 11, no. 1, pp. 48–60, Feb. 2004.

[9]. T. Alpcan and T. Basar, Network Security: A Decision and Game Theoretic Approach. Cambridge University Press, 2010.

[10]. X. Liang and Y. Xiao, “Game theory for network security,” IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 472–486, 2013.

[11]. H. Bedi, S. Roy, and S. Shiva, “Game theory-based defense mechanisms against ddos attacks on TCP/TCP-friendly flows,” in Proc. 2011 Computational Intelligence Cyber Security, pp. 129–136.

[12]. A. Patcha and J. M. Park, “A game theoretic formulation for intrusion detection in mobile ad hoc networks,” Int’l J. Netw. Security, vol. 2, no. 2, pp. 131–137, 2006.

[13]. E. A. Panaousis and C. Politis, “A game theoretic approach for securingAODV in emergency mobile ad hoc networks,” in Proc. 2009 IEEE Conf. Local Comput. Netw., vol. 53, pp. 985–992.

[14]. J. Omic, A. Orda, and P. Van Mieghem, “Protecting against network infections:a game theoretic perspective,” in Proc. 2009 IEEE INFOCOM, pp. 1485–1493.

[15]. N. Santosh, R. Saranyan, K. Senthil, and V. Vetriselvi, “Cluster based cooperative game theory approach for intrusion detection in mobile ad-hoc grid,” in Proc. 2008 International Conf. Advanced Comput. Commun., pp. 273–278.

[16]. F. Li, Y. Yang, and J. Wu, “Attack and flee: game-theory-based analysis on interactions among nodes in MANETs,” IEEE Trans. Syst., Man, Cybern. (B), vol. 40, pp. 612–622, June 2010.

[17]. M. Huang, P. Caines, and R. Malhame, “The NCE (mean field) principle with locality dependent cost interactions,” IEEE Trans. Auto. Control, vol. 55, no. 12, pp. 2799–2805, Dec. 2010.

[18]. M. Y. Huang, “Mean field stochastic games with discrete states and mixed players,” in Proc. 2012 GameNets.

[19]. F. Meriaux, V. Varma, and S. Lasaulce, “Mean field energy games in wireless networks,” in Proc. 2012 Asilomar Conf. Signals, Syst., Comput.

[20]. H. Tembine, P. Vilanova, M. Assaad, and M. Debbah, “Mean field stochastic games for SINR-based medium access control,” in Proc. 2011 Int’l ICST Conf. Performance Evaluation Methodologies Tools.

[21]. D. Zheng, H. Tang, and F. R. Yu, “Game theoretic approach for security and quality of service (QoS) co-design in MANETs with cooperative communications,” in Proc. 2012 MILCOM.

[22]. M. Puterman, Markov Decision Processes. John Wiley, 1994.

[23]. C. Liang and K. R. Dandekar, “Power management in MIMO ad hoc networks: a game-theoretic approach,” IEEE Trans. Wireless Commun., vol. 6, no. 4, pp. 2866–2882, Apr. 2007.

[24]. H. Zhang, O. Kreidl, B. DeCleene, J. Kurose, and X. Ni, “Security analysis of the bootstrap protocol for deny-by-default mobile ad-hoc networks,” in Proc. 2009 MILCOM.

[25]. A. Attar, H. Tang, A. Vasilakos, F. R. Yu, and V. Leung, “A survey of security challenges in cognitive radio networks: solutions and future research directions,” Proc. IEEE, vol. 100, no. 12, pp. 3172–3186, 2012.