Mixed and Continuous Strategy Monitor-Forward Game Based Selective Forwarding Solution in WSN

Hongmei Liao and Shifei Ding

1School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China
2Key Laboratory of Intelligent Information Processing, Institute of Computing Technology, Chinese Academy of Science, Beijing 100190, China

Correspondence should be addressed to Shifei Ding; dingsf@cumt.edu.cn

Received 24 July 2015; Accepted 1 November 2015

Copyright © 2015 H. Liao and S. Ding. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless sensor networks are often deployed in unattended and hostile environments. Due to the resource limitations and multihop communication in WSN, selective forwarding attacks launched by compromised insider nodes are a serious threat. A trust-based scheme for identifying and isolating malicious nodes is proposed and a mixed strategy and a continuous strategy Monitor-Forward game between the sender node and its one-hop neighboring node is constructed to mitigate the selective dropping attacks in WSN. The continuous game will mitigate false positives on packet dropping detection on unreliable wireless communication channel. Simulation results demonstrate that continuous Monitor-Forward game based selective forwarding solution is an efficient approach to identifying the selective forwarding attacks in WSN.

1. Introduction

Wireless sensor networks have been used in a wide range of applications such as military provision, environment monitoring, and man-unreachable circumstances [1–3]. Due to their shared medium, multihop relay, and lack of physical protection, nodes are vulnerable to various routing attacks, such as selective forwarding, black hole, wormhole, and sinkhole attacks. In these attacks, selective forwarding of packets [4] becomes an increasingly important concern as it is difficult to do with many current techniques in WSNs. As continuously misbehaving nodes in WSN will be distrusted and excluded from the network soon, a rational potential attacker will act normally most of the times, occasionally dropping packets. A number of literatures [5–9] are proposed to overcome this problem. However, this literalness focuses on cooperation among nodes in a WSN. In these researches, selfish nodes drop packets only to conserve their resources but not to damage the whole networks. References [10–21] proposed multipath schemes to eliminate the selective forwarding attack and enable energy to be balanced among these paths in a WSN. However, the adversary can overhear the communication between nodes in WSN and can modify routing control packets affecting the discovery of alternative paths and creating routing loops and dead ends. Multipath incurs more energy consumption than single-path routing. In particular, when a node is captured and compromised, all information of the node, including any security keys, becomes available to the attackers, and the adversary will have full control of the node. Game theory [22] is one of the effective mathematical methods to solve the attacker-defender interaction problems. And there is growing interest in using game to solve selective forwarding attack analysis problems. In [23], they analyze the collusion in selective forwarding attacks and propose a multiattacker repeated colluding game. They think the colluding attackers form a malicious group and the punishment to each colluding attacker is strongly related to the overall performance of this malicious group. In [24], the mixed strategy Nash equilibrium of the game provides the probability that the flooding packet would be forwarded by the receiver node. Here node \(i\) needs to make a decision whether to forward \(p\) or not. The number of players of the game is the number of nodes that receive \(p\). Only a limited number of neighbors of the source node participate...
in forwarding. In [25], a stationary Markovian game model is utilized to optimize system performance in terms of throughput, delay, and power consumption cost. However, in Markov games, actions of players are determined based on the current state of the game, instead of considering the complete game history. In [26], they present a systematic study of collusion-resistant routing in noncooperative wireless ad hoc networks. In their model, each node in a path receives a payment from source node $S$ for each forwarded packet. A central authority collects payments from the source node and guarantees secure distribution of payments to the forwarding nodes. And they assume that packet discarding and standby consume much less energy. However, this centralized mechanism and the above assumption are not suitable in WSN. Literature [27] proposed a generalized two-hop $f$-cast relay for packet routing, where $f$ is replicated packet redundancy limit. They explore possible maximum throughput capacity of a node and determine the corresponding optimal setting of $f$ to achieve it. Node’s payoff is the achievable throughput capacity of its own traffic. And all nodes play the symmetric strategy profiles. Literature [28] proposes a model based on game theory and graph theory to investigate equilibrium conditions of packet forwarding strategies. In [28], they combine downstream assessments and end-to-end assessments to detect and mitigate collaborative Grey hole attacks. And a two-hop acknowledgment mechanism is integrated with forwarding assessments. However, in [6, 28], they assume the channel is error-free wireless and no per-link encryption. This does not meet the actual situation of most WSNs. In literature [29], they develop a channel aware detection (CAD) algorithm that can effectively identify the selective forwarding misbehavior from the normal channel losses. In [30], the authors proposed a packet forwarding framework based on each node’s own past actions and its observation of other nodes. However, their objective is to maximize the node’s own payoff, not to cause damage to other nodes. In literature [31], to obtain the trust value of the insider nodes along the route $x$, after every $M$ data packets, the sender will generate a check packet and send it to destination node thought the route $x$. As this check packet passes through the route $x$, each insider node in $x$ will attach its opinions about its upstream and downstream neighbors to the check packet. However, this mechanism cannot solve bad mouthing attack when nodes attach their opinions to the check packets. Selective dropping attack launched by insider node is still a problem that needs to be solved.

A repeated continuous noncooperative game based neighbor monitoring system to detect compromised nodes in selective forwarding attack in WSN is proposed in this paper. Based on the monitoring results, we can select more reliable cluster heads having sufficient residual energy and high trust level for data forwarding and data aggregation.

The rest of this paper is organized as follows. Game theory is introduced in Section 2. In Section 3, a mixed strategy Monitor-Forward game in WSN is constructed and simulated. In Section 4, a game with continuous strategy to mitigate false positives on packet dropping detection on unreliable wireless communication channel is constructed and simulated. Routing protocol without monitor mechanism and routing protocol with mixed strategy Monitor-Forward game and with continuous strategy Monitor-Forward game in a clustered WSN are all simulated and compared in Section 5. Finally, conclusions are drawn in Section 6.

2. Game Theory

Game theory is the study of problems of conflict and cooperation among independent decision-makers. Game theory is one of the effective mathematical methods to solve the attacker-defender interaction problems in WSN. In game theory, pure strategy means that the players choose strategies determinedly. However, in the real case, the rational node will change its strategy over time. In action decision of WSN, if the suspicious node always monitors his neighbor node, too much energy will be consumed. As a result, rational suspicious node will selectively drop the packets it received with certain probability and pretends to be legitimate sometimes and the monitoring node will monitor its next hop node with certain probability also.

2.1. Mixed Strategy Nash Equilibrium. Mixed strategy allows a player to randomly select a pure strategy. We first construct the Monitor-Forward game as a mixed strategy game, in which the node’s strategy is probability distribution over its pure strategy set. A pure strategy can be regarded as a degenerate case of a mixed strategy, in which that particular pure strategy is selected with probability 1 and every other strategy with probability 0.

A Nash equilibrium for a mixed strategy game is stable if a small change in probabilities for one player leads to a situation where two conditions hold:

(i) The player who did not change has no better strategy in the new circumstance.
(ii) The player who did change is now playing with a strictly worse strategy.

2.2. Continuous Strategy Game. A continuous game allows more general sets of pure strategies, which may be uncountable infinite. It extends the notion of a discrete game, where the players choose from a finite set of pure strategies. In general, a game with uncountable infinite strategy sets will not necessarily have a Nash equilibrium solution. If, however, the strategy sets are required to be compact and the utility functions continuous, then a Nash equilibrium will be guaranteed.

The existence of a Nash equilibrium for any continuous game with continuous utility functions can be proven using Irving Glicksberg’s generalization of the Kakutani fixed point theorem.

2.3. Repeated Game and QRE of a Repeated Game. In game theory, a repeated game is a special case of dynamic game which consists in some number of repetitions of some base game (called a stage game). It captures the idea that a player will have to take into account the impact of his current...
action on the future actions of other players; this is called his reputation.

The stage game in our repeated game in WSN is the 2-person games played by the suspicious node $N_s$ and the monitoring node $N_m$. The formal definition is as follows.

**Formal Definition.** For $G$-period repeated game, at each period $g$, the moves during periods $1, \ldots, g-1$ are known to every player. Suppose $\delta$ is the total discounted payoff for each player is computed by

$$
\sum_{g=1}^{G} \delta^{g-1} U_i(g),
$$

where $U_i(g)$ denotes the payoff to player $i$ in period $g$.

If $G = \infty$, the game is referred to as the infinitely repeated game. The average payoff to player $i$ is then given by

$$
\bar{U}_i = (1 - \delta) \sum_{g=1}^{\infty} \delta^{g-1} U_i(g).
$$

In our model, $N_m$ is player 1 and $N_s$ is player 2. The player will get punishment from other players in the near future if it acts greedily. Therefore, the player (node $N_m$ and node $N_s$) will focus more on the long-term overall utility than the one-shot utility on one stage of the game. From Folk Theorem, for an infinitely repeated game, if a feasible outcome gives each player better payoff, the Nash equilibrium can be obtained.

However, because of the limited energy of nodes in WSN, the Monitor-Forward game is indeed a random ended repeated Monitor-Forward game. Random repeated game is very different from finite games with definite end time in action or strategy choosing. But it is very similar to infinite games in strategy choosing. So, we can treat this game as infinite games in strategy analysis process.

In a multi-round repeated game, the nodes will focus more on the long-term overall utility. Since the game is ended randomly, node's lifetime which is decided by the residual battery energy is important in the strategy choosing. Suppose $\omega$ denotes how long the suspicious node and monitoring node believe the repeated Monitor-Forward game will last. $\omega$ is denoted by a real number that lies in the interval $(0, 1)$. $\omega_0$ is a threshold in the interval $(0, 1)$. In each stage of the repeated game,

1) if $\omega > \omega_0$—that is, the suspicious node $N_s$ and the monitoring node $N_m$ believe that the game will repeat for many stages—each node will always choose its mixed strategy based Nash equilibrium $x_m^*$, $x_s^*$ to maximize the long-term overall utility in the future.

2) if $\omega < \omega_0$, we think the residual battery energy of monitoring node $N_m$ or $N_s$ is not enough and Cluster Rotation Algorithm will be executed soon. To maximize its profit, $N_s$ will be violated from the Nash equilibrium strategy and choose to drop the packet fearlessly to maximize its one-shot utility in the current stage.

2.4. Quantal Response Equilibrium. With the Monitor-Forward game repeats, the nodes obtains more and more information of the other's misbehavior. We can obtain the Quantal response equilibrium (QRE) by utilizing the method in [32]. Players make choices based on a quantal-choice model and assume other players do so as well.

Quantal response equilibrium (QRE) is a solution concept in game theory. First introduced by Richard McKelvey and Thomas Palfrey, it provides an equilibrium notion with bounded rationality. In a quantal response equilibrium, players are assumed to make errors in choosing which pure strategy to play. The probability of any particular strategy being chosen is positively related to the payoff from that strategy. Quantal responses are smoothed-out best responses, in the sense that players are more likely to choose better strategies than worse strategies but do not play a best response with a probability one.

By far the most common specification for QRE is logit equilibrium (LQRE) [32]. In a logit equilibrium, player's strategies are chosen according to the probability distribution:

$$
P_{ij} = \frac{\exp(\lambda EU_{ij}(P_{-i}))}{\sum_k \exp(\lambda EU_{ik}(P_{-i}))},
$$

where

(i) $P_{ij}$ is the probability of player $i$ choosing strategy $j$;

(ii) $EU_{ij}(P_{-i})$ is the expected utility to player $i$ of choosing strategy $j$ given other players are playing according to the probability distribution $P_{-i}$;

(iii) $\lambda$ is a rationality parameter which is nonnegative (sometimes written as $1/\mu$). As $\lambda \to 0$, players become "completely irrational" and play each strategy with equal probability. As $\lambda \to \infty$, players become "perfectly rational" and play approaches a Nash equilibrium. So LQRE will always be at least as good a fit as Nash equilibrium. Changes in the parameter can result in large changes to equilibrium behavior.

3. Mixed Strategy Game Based Monitoring Mechanism in WSN

3.1. A Monitoring Based Trust System. In WSNs, compromised nodes have legitimately registered into the network and the attackers can bypass the public key and private key system. A reputation-based trust system which maintains information about nodes’ history behaviors is a necessary complement to the existing security mechanism.

Trust is a particular level of the subjective probability with which an agent assesses another node in a context such as data integrity, honesty, and packet forwarding. In this paper, we suppose that in a clustered wireless sensor network, the cluster heads aggregate and compress the data from the sensor nodes in the cluster and forward it to its next-hop cluster head or the base station and only the trust on selective forwarding context is considered in the Monitor-Forward game. Cluster heads are also in charge of trust values on
data reliability of sensor nodes in these clusters. A distributed watch dog runs on every cluster head in WSN to monitor and record the packet forwarding behaviors of its next hop cluster head in the route to destination. Each cluster head node in WSN maintains its own neighbor set \( N_N \) and a set of neighbor nodes towards the sink FN. FN is a subset of \( N_N \). It will select a node in FN with highest trust value on packet forwarding. If the suspicious node forwards the packet correctly, its trust value stored in the monitoring node will increase. Nodes with low trust value will then be excluded from the network. Node transceivers are supposed to be omnidirectional and neighboring overhearing is feasible in our model.

Each cluster head executes the trust model by monitoring its neighboring nodes’ participation in the packet forwarding mechanism. If the node forwards the packet, it confirms that the node has acted in a benevolent manner and so its direct trust counter is incremented. If the forwarding node does not transmit the packet, its corresponding direct trust measure is decremented. In [33], after transmitting the packet, sending node must wait a trust update interval until the time it overhears the retransmission by its neighbor or the trust update interval has expired. This interval is related to the mobility and traffic of the network and can be set accordingly. If during the TUI the node is able to overhear its neighboring node retransmit the same packet, the sending node increases the trust value for that neighbor. In case no retransmission is heard and a time-out occurs when the TUI expires, the trust value for that neighbor is decremented. However, after transmitting the packet, the persistent monitoring of sending node would cost too much energy. In order to solve this problem, we propose a low cost game based monitoring mechanism to detect the compromised node.

3.2. A Monitor-Forward Game Based Monitoring Mechanism in WSN. In WSN, the sensor node consumes power for sensing, communicating, and data processing. More energy is required for communication than any other process. The transceiver of a node has four operational states that are transmit, receive, idle, and sleep. Most transceivers operating in idle mode consume almost equal power to operate in receive mode [34]. Thus, in a lot of literature, the transceiver is completely shut down when it is not transmitting or receiving rather than being in the idle or listening mode. In [33], to monitor the neighbor node, after transmitting the packet, sending node will not go to sleep but waits a trust update interval until it overhears the retransmission by its neighbor or the trust update interval has expired. However, if the trust update interval is too short, the transmission of its neighbor will be missed; if trust update interval is long, the persistent monitoring of node will cost a lot of energy.

By traffic analysis and statistical analysis executed in end nodes of a path [35], we can detect anomalies in network traffic and calculate probability of occurrence of attack on the path. However, which node in this path is malicious is not known. Nodes with monitoring mechanism can detect selective dropping attack of their neighboring node.

3.3. Formal Definition of the Game. The formal definition of the game is as follows.

\[ G = \langle N, S, f \rangle \]

where \( N \) is the set of players, \( N_m \) denotes the monitoring node and \( N_i \) denotes the suspicious node; \( S_m \) denotes the strategy set for the monitoring node; \( S_i \) denotes the strategy set for the suspicious node; \( S = S_m \times S_i \) is the set of strategy profiles of the game; \( f = (f_m(x), f_i(x)) \) is the payoff function for \( x \in S \), where \( x = (x_m, x_i) \), \( x_m \in S_m \), and \( x_i \in S_i \).

Let \( x_m \) be a strategy profile of node \( N_m \) and let \( x_i \) be a strategy profile of node \( N_i \). Node \( N_m \) will obtain payoff \( f_m(x) \) when it chooses strategy \( x_m \) and \( N_i \) chooses strategy \( x_i \), resulting in strategy profile \( x = (x_m, x_i) \).

A strategy profile \( x^* \in S \) is a Nash equilibrium (NE) if each rational node selects its best possible response to the other node’s strategies provided that neither node can increase its utility by unilaterally changing its own strategy. That is,

\[
\begin{align*}
&f_m(x_m^*, x_i^*) \geq f_m(x_m, x_i^*) \quad x_m \in S_m, \\
&f_i(x_i^*, x_m^*) \geq f_i(x_i, x_m^*) \quad x_i \in S_i.
\end{align*}
\]

By traffic analysis and statistical analysis executed in end nodes of a path [36], we can detect anomalies in network traffic and calculate probability of occurrence of attack on the path. However, if the neighboring node forwards the packet to its coconspirators, monitoring mechanism without collusion considering will not detect this attack. Thus, nodes with normal reputation in a path whose attack probability is greater than a certain threshold will use two-stage dynamic game with collusion considering.

Considering the larger cost of collusion attack monitoring, the nodes in the path whose attack probability is below the threshold will play a simpler static game without collusion considering. We begin with the simpler Monitor-Forward game without collusion considering.

3.4. Pure Strategies Set of the Game. The static Monitor-Forward game without collusion considering is a simultaneous game. In this game, each player has a finite number of pure strategies. The suspicious node \( N_i \) has two strategies: Forward Packet \((F)\) and Drop Packet \((D)\). That is to say, the strategies set of \( N_i : S_i = \{F, D\} \). The monitoring node \( N_m \) has two strategies: Listen \( L \) time \((L)\) and go to Sleep \((S)\). The strategies set of \( N_m : S_m = \{L, S\} \), where \( L \) is the length of monitoring time. We set \( L \) which is equal to the average round-trip time (RTT) of one hop distance in WSN.

3.5. Mixed Strategy Nash Equilibrium of the Monitor-Forward Game. Suppose in this mixed strategy game the suspicious node’s strategy is a probability distribution \([p, 1 - p]\) over its possible action set \([F, D]\). Variables \( p, 1 - p \) are the probabilities for the suspicious node adopting Forward Packet \((F)\) and Drop Packet \((D)\), respectively. On the contrary, for the monitoring node, its strategy is a probability distribution \([h, 1 - h]\), over its action set \([M, S]\). Here \( h, 1 - h \) are
The mixed strategy allows a player to randomly select a pure strategy. And the Nash equilibrium of the game indicates the outcome in which neither suspicious node nor the monitoring node wants to unilaterally change its strategy.

3.6. Result of Simulation. As we have known, \( l \) is the multiple of average RTT of one hop transmission in WSN and we suppose \( l = 1 \) in the static game. For simplicity, we set \( E_{\text{monitor}} = 2; E_{\text{forward}} = 1 \). Figure 1 shows the payoff matrix of the Monitor-Forward game.

Figure 1(a) shows the payoff matrix with \( B = 1 \) and \( C = 2 \). The Nash equilibrium is as follows:

\[
N_m : \{ h, 1-h \} = \{1.00000, 0.00000 \}. \text{ Expected payoffs} = 0.
\]
\[
N_s : \{ p, 1-p \} = \{0.00000, 1.00000 \}. \text{ Expected payoffs} = 1.0.
\]

Figure 1(b) shows the payoff matrix with \( B = 4 \) and \( C = 5 \). The Nash equilibrium is as follows:

\[
N_m : \{ h, 1-h \} = \{0.85714, 0.14286 \}. \text{ Expected payoffs} = 1.0.
\]
\[
N_s : \{ p, 1-p \} = \{1.00000, 0.00000 \}. \text{ Expected payoffs} = -1.0.
\]

If we set \( B = C = 5 \), the loss of the suspicious node is the same as the gain of the monitoring nodes; we call this game a zero-sum game.

Figure 1(c) shows the payoff matrix with \( B = 5 \) and \( C = 5 \). This is a zero-sum game too.

The Nash equilibrium is as follows:

\[
N_m : \{ h, 1-h \} = \{0.75000, 0.25000 \}. \text{ Expected payoffs} = 1.0.
\]
\[
N_s : \{ p, 1-p \} = \{1.00000, 0.00000 \}. \text{ Expected payoffs} = -1.0.
\]

Figure 1(d) shows the payoff matrix with \( B = 7 \) and \( C = 5 \). The Nash equilibrium is as follows:

\[
N_m : \{ h, 1-h \} = \{0.60000, 0.40000 \}. \text{ Expected payoffs} = 1.0.
\]
\[
N_s : \{ p, 1-p \} = \{1.00000, 0.00000 \}. \text{ Expected payoffs} = -1.0.
\]
From the above simulation results, we can see that higher punishment $B$ will lead to smaller monitoring probability of the monitoring node $N_m$ and smaller expected payoffs of the suspicious node $N_s$. However, in the real case, packet loss, data corruption, and variable propagation delays will lead to large amounts of false positives on packet dropping detection that rely on strict timing. Thus, too large $B$ is not suitable for the unreliable wireless communication channel in WSN. The parameter setting should take the real-time channel quality into account. A balance between the severe punishment and avoiding false positives on packet dropping detection is needed.

3.7. QRE Simulation Result of the Repeated Game. We conducted an experiment with $E_{\text{monitor}} = 2$, $E_{\text{forward}} = 1$, $l = 1$, $B = 5$, and $C = 5$, where nodes played the Monitor-Forward game without collusion consideration illustrated in Figure 1(c); the QRE of repeated game is shown in Figure 2.

The experiment parameters are $E_{\text{monitor}} = 2$, $E_{\text{forward}} = 1$, $l = 1$, $B = 7$, and $C = 5$, where nodes played the Monitor-Forward game without collusion consideration illustrated in Figure 1(d) firstly. The QRE of the repeated game is shown in Figure 3.

By using the method described in detail in [32], we can obtain predicted frequencies of moves at each information set for any parameter, $\lambda$, of the AQRE model. Given a data set from the particular experimental game, the estimate, $\hat{\lambda}$, is the value of $\lambda$ that maximizes the likelihood of that data set.

4. Continuous Strategy Monitor-Forward Game in WSN

4.1. Unreliable Communication Channel. Because of the unreliable wireless communication channel in WSN, packet loss, data corruption, and variable propagation delays will lead to large amounts of false positives on packet dropping detection that rely on strict timing. Normal loss events such as medium access collision or bad channel quality will lead to normal loss rates which are not caused by malicious act. The normal loss rates $p_i$ can be computed by the following formula:

$$p_i = p_b + p_m - p_b \cdot p_m,$$

where $p_m$ denotes the packet loss rate due to bad channel quality and $p_b$ denotes the packet loss rate due to medium access collisions. The detail computing of $p_m$ and $p_b$ can be found in literature [37]. Nodes may be considered to be compromised due to a packet propagation delay or normal packets loss. However, if the monitoring time is set as twice the RTT or longer, the power consumption will be significant. So, we construct a continuous game which allows players to choose a strategy from a continuous strategy set. Monitoring node has numerous possible actions to choose from in this continuous game.

4.2. Continuous Monitor-Forward Game in WSN. As previously mentioned, a mixed strategy Nash equilibrium is equivalent where at least one player is playing a mixed strategy. In the continuous Monitor-Forward game $G = (N, S, f)$, suspicious node $N_s$ has two pure strategies: Forward Packet ($F$) and Drop Packet ($D$). That is to say, the strategies set of $N_s$ is $S_s = \{F, D\}$. The monitoring node $N_m$’s strategy is monitoring $IT$ time which is denoted by $M(IT)$, where $M(IT)$ is continuous strategy. $T$ denotes the average round-trip time (RTT) of one hop distance in WSN and $l$ is the multiple of RTT. $l \in [0, k]$, where $K$ is the upper limit of $l$.

We should take into account of normal packet losses due to poor channel quality and medium access collisions by setting different $k$ in the Monitor-Forward game. As wireless loss probability due to bad channel quality varies with the network status changing, $k$ is dynamically adjusted with the normal loss rates in the game every time the game is played.

By the continuous game theory, we know that the utility functions of a player with continuous strategy are often expressed by a quadratic equation of a variable. As $E_{\text{monitor}}$ is...
the energy consumption of node $N_S$ monitoring its next hop last for one RTT, the utility of node $N_m$ due to monitoring is $-l^2 \cdot E_{\text{monitor}}$. If $N_f$ forwarded the packet, node $N_m$ will gain $E_{\text{forward}} \cdot l$, which is lost by node $N_S$. If $N_f$ dropped the packet, node $N_m$ will punish $N_f$ with $B$ and $N_f$ will obtain $C$ from the opponent of $N_m$. The gain of node $N_m$ from the punishment is in direct proportion to $l^2/k$ and the utility of $N_m$ from its opponent's award to $N_f$ is $C \cdot k$. So, we can define the utility function $f_m(x)$, which is $f_m(x_m, x_s)$, of the monitoring node $N_m$ as

$$f_m = -l^2 E_{\text{monitor}} + p \cdot (E_{\text{forward}}) \cdot l + (1 - p) \cdot \left(\frac{B \cdot l^2}{k} - C \cdot k\right),$$

where variables $p, 1 - p$ are the probabilities for the suspicious node adopting Forward Packet $(F)$ and Drop Packet $(D)$, respectively. As we can see from this formula, the gain for monitoring is in proportion to the length of monitoring time $l$ and the loss for short monitoring is in inverse proportion to $l$. When $l \rightarrow k$, we think the false positives on packet dropping detection are negligible; $B \cdot l^2/k \rightarrow B$.

Define the utility functions $f_s(x_m, x_s)$ of $N_s$ as

$$f_s = \begin{cases} \hat{F} E_{\text{monitor}} - \frac{B \cdot l^2}{k} + C \cdot k & x_s = D \\ -E_{\text{forward}} + l^2 E_{\text{monitor}} & x_s = F. \end{cases}$$

4.3. Best Response Function of the Continuous Game. A best response is the point at which each player in a game has selected the best response (or one of the best responses) to the other players’ strategies.

To achieve a strategy Nash equilibrium, set

$$p \cdot E_{\text{forward}} + (1 - p) \cdot C = -E_{\text{monitor}} + p \cdot (E_{\text{forward}}) \cdot l + (1 - p) \cdot \left(\frac{B \cdot l^2}{k} - C \cdot (k - l)\right)$$

$$E_{\text{monitor}} - \frac{B \cdot l^2}{k} + C \cdot (k - l) = -E_{\text{forward}} + l^2 E_{\text{monitor}}.$$  

In this continuous game, the best response of $N_m$ to $N_s$’s strategies is setting monitoring time $l$ which meets $f_m = \max f_m$ and this can be substituted into its maximization problem.

We have known that

$$f_m = -l^2 E_{\text{monitor}} + p \cdot (E_{\text{forward}}) \cdot l + (1 - p) \cdot \left(\frac{B \cdot l^2}{k} - C \cdot k\right).$$

Then,

$$\max(f_m(l)) = \max \left( -E_{\text{monitor}} \cdot \frac{B}{k} - B \cdot \frac{p}{k} \cdot l \right)$$

$$- (1 - p) C \cdot k + p \cdot E_{\text{forward}} \cdot l.$$  

For fixed $p$, if $-E_{\text{monitor}} + B/k - B \cdot p/k \geq 0$—that is, $p \leq 1 - E_{\text{monitor}} \cdot k/B - N_m$’s best response is $l = k$.

If $p > 1 - E_{\text{monitor}} \cdot k/B$, set the first partial derivative of the payoff function to be equal to zero with respect to $N_m$’s strategy variable $l$:

$$\frac{\partial f_m}{\partial l} = 2 \cdot \left( -E_{\text{monitor}} \cdot \frac{B}{k} - B \cdot \frac{p}{k} \cdot l + p \cdot E_{\text{forward}} \right) = 0.$$  

And we can find that $N_m$’s best response function is

$$l(p) = \frac{(p \cdot E_{\text{forward}})}{(2 \ast (E_{\text{monitor}} - B/k + B \cdot p/k))}.$$  

For $N_f$, which have two discrete strategies, set $f_s(D) = f_s(F)$. That is,

$$l^2 E_{\text{monitor}} - \frac{B \cdot l^2}{k} + C \cdot k = -E_{\text{forward}} + l^2 E_{\text{monitor}}.$$  

Solve this equation:

$$l^* = \frac{k \cdot \left(E_{\text{forward}} + \sqrt{E_{\text{forward}}^2 + 4 \cdot B \cdot C}\right)}{(2 \cdot B)}.$$  

Feeding $l^*$ into $N_m$’s best response function, $(l^*, p^*)$ is the Nash equilibrium of this continuous game.

4.4. Simulation of the Continuous Monitor-Forward Game. In this continuous game, we have known that $f_m = -l^2 E_{\text{monitor}} + p \cdot (E_{\text{forward}}) \cdot l + (1 - p) \cdot \left(\frac{B \cdot l^2}{k} - C \cdot k\right)$. Set $E_{\text{monitor}} = 2$, $E_{\text{forward}} = 1, B = 7, C = 5$, and $k = 2$; The payoff function of the monitoring node $N_m$ is illustrated as in Figure 4. $N_m$’s payoff (in the $y$-axis) is a function of the length of monitoring time $l$ that $N_m$ last (in the $x$-axis). Figures 4(a)–4(d) graphs this payoff function of $N_m$ on different forward probability $p$ of the suspicious node $N_f$ to its next hop.

$N_m$’s best response function $l(p) = (p \cdot E_{\text{forward}})/(2 \ast (E_{\text{monitor}} - B/k + B \cdot p/k))$ is shown in Figure 5. The line in Figure 5 shows the length of monitoring time $l$ that $N_m$ last (in the $y$-axis), as a function of the probability that $N_f$ plays “Forward” (shown in the $x$-axis).

By setting $f_s(D) = f_s(F)$, we can obtain

$$l^* = \frac{k \cdot \left(E_{\text{forward}} + \sqrt{E_{\text{forward}}^2 + 4 \cdot B \cdot C}\right)}{(2 \cdot B)}$$

$$= 1.8392.$$
Feeding $l^*$ into $N_m$'s best response function, $(l^*, p^*) = (1.8392, 0.4647)$ is the Nash equilibrium of the continuous game.

As we can see, if the punishment $B$ is small, the game will result in an equilibrium with low forward probability $p$ of $N_s$.

5. Simulation of a Routing Protocol with Monitor-Forward Game in a Clustered WSN

5.1. Simulation Setup. The routing protocol with mixed strategy Monitor-Forward game (MSMFM) and routing protocol with continuous strategy Monitor-Forward Game (CSMFM) are simulated in various setups using Matlab. 100 nodes are randomly distributed in an area of 100-by-100 meters and the base station is set in the center of the area.

Initial energy of each node is set to 0.5 joules. The election probability of a node to become cluster head is 0.1. The battery power consumption of $N_m$ to monitor its next hop node $N_s$ for one RTT is $E_{\text{monitor}} = 0.0000001$ joules. The energy consumption of $N_s$ to forward the packet it received to its next hop is $E_{\text{forward}} = 0.00000005$ joules. The punishment $B$ for the dropping packet of $N_s$ is set to 0.00000035 and the suspicious node’s illegal gain $C$ from the adversary of the network which has compromised inside attackers is 0.00000025. The game is repeated 9999 rounds. The traffic is generated randomly.

5.2. Simulation Numerical Analysis. The initial deployment of the routing protocol without monitor mechanism (WMM) is shown as in Figure 6(a). 100 nodes are randomly distributed in an area of 100-by-100 meters and the base station is set in the center of the area. $r$ denotes the packet transmitting round in WSN. As we can see in Figure 6, the first node died in the round $r = 999$ and all nodes in the area died in the round $r = 4500$. 
The length of monitoring time $l$ that $N_m$ last

$N_m$'s best response to probability $p$ that $N_s$ plays "Forward".

**Figure 5:** $N_m$’s best response to the probability $p$ that $N_s$ plays “Forward”.

(a) The initial deployment

(b) The first node which died in the round $r = 999$

(c) All nodes which died in the round $r = 4500$

**Figure 6:** The initial deployment and lifetime of WMM.
In the ideal case without normal loss, 15% of the cluster
head nodes are randomly chosen as selective dropping
attackers in the forwarding paths between source and desti-
nation pairs. The network lifetime using different protocols is
illustrated in Figure 7.

The simulation results indicate that lifetimes of networks
using MSMFM and CSMFM are shorter than WMM as they
have monitor mechanism which consumes much energy.
Compared with MSMFM, CSMFM which use continuous
strategy extends the lifetime of the network, delays the first
node’s death time, and enhances the energy efficiency.

The packet forward probability without normal packet
loss is shown in Figure 8. The Packet Delivery Radio of
CSMFM and MSMFM is improved compared to WMM
because they detect and isolate the attacker and forward
the packets to the destination through a different secure
path. Using WMM which have no monitor mechanism, there
is a significant degradation in the Packet Delivery Radio
with selective dropping attacks. Using MSMFM, the Packet
Delivery Radio is improved to 85% in the case of 20%
dropping and 65% in case of 50% dropping. Using CSMFM,
the Packet Delivery Radio is improved to 88% in the case of
20% dropping and 70% in case of 50% dropping.

The curves in Figure 9 illustrate the performance of
CSMFM, MSMFM, and WMM in the presence and absence
of attacker(s) with normal losses. As the sum of false alarm
and missed detection probabilities of CSMFM is degraded
compared to MSMFM, the Packet Delivery Radio of CSMFM
is increased. And the increased channel loss rate does cause
more packet loss.

6. Conclusion

Due to the resource limitations and open environments in
WSN, traditional cryptography based security mechanisms
such as authorization and authentication are not effective
against insider attacks. To mitigate selective forwarding attacks launched by insider nodes in multihop communication, a repeated mixed strategy and an energy-efficient continuous strategy Monitor-Forward game between the sender node and its one-hop neighboring node in a cluster WSN are proposed and simulated. We propose a trust management mechanism to identify and isolate malicious nodes for the cluster wireless sensor networks. A distributed watch dog runs on every cluster head in WSN to monitor and record the packet forwarding behaviors of its next hop cluster head node. By this trust model, we can select more reliable cluster heads having sufficient residual energy and high trust level.

The main contributions of our work are as follows:

1. We constructed and simulated a mixed strategy Monitor-Forward game, analyze the payoff matrix and mixed strategy Nash Equilibrium of the game with different parameters: B and C. The random

ended repeated mixed strategy game and its quantal response equilibrium are discussed.

2. Because of the unreliable wireless communication channel in WSN, packet loss, data corruption, and variable propagation delays will lead to large amounts of false positives on packet dropping detection that rely on strict timing. We constructed and simulated a continuous game which allows players to choose a strategy from a continuous strategy set.

3. Routing protocol without monitor mechanism, routing protocol with mixed strategy Monitor-Forward game, and routing protocol with continuous strategy Monitor-Forward game in a clustered WSN are all simulated and analyzed with Matlab in various setups. Game analyzing and simulation results demonstrate that game theory based framework is an efficient approach to identifying the selective forwarding

Figure 9: The performance of CSMFM, MSMFM, and WMM in the presence and absence of attacker(s) with normal losses.
attacks and increase the packets forward probability of the networks. Continuous strategy game will consume less battery energy and have less false alarms than mixed strategy game on unreliable channels.

Conflict of Interests
The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment
This paper is supported by the Fundamental Research Funds for the Central Universities (2014XT04).

References

[1] Z. Li, M. Li, and Y. Liu, “Towards energy-fairness in asynchronous duty-cycling sensor networks,” ACM Transactions on Sensor Networks, vol. 10, no. 3, article 38, 2012.

[2] Y. Liu, Y. He, M. Li, J. Wang, K. Liu, and X. Li, “Does wireless sensor network scale? A measurement study on GreenOrbs,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 10, pp. 1983–1993, 2013.

[3] P. Chen, H. Ma, S. Gao, and Y. Huang, “Modified extended kalman filtering for tracking with insufficient and intermittent observations,” Mathematical Problems in Engineering, vol. 2015, Article ID 981727, 9 pages, 2015.

[4] H.-M. Sun, C.-M. Chen, and Y.-C. Hsiao, “An efficient countermeasure to the selective forwarding attack in wireless sensor networks,” in Proceedings of the IEEE Region 10 Conference (TENCON ’07), pp. 1–4, Taipei, Taiwan, October 2007.

[5] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, D. K. Sanyal, R. Neogy, and S. Pal, “A novel incentive based scheme to contain selective forwarding in wireless sensor network,” in Computer Information Systems and Industrial Management, vol. 8104 of Lecture Notes in Computer Science, pp. 301–312, 2013.

[6] M. Félegyházi, J.-P. Hubaux, and L. Buttyán, “Nash equilibria of packet forwarding strategies in wireless ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 5, no. 5, pp. 463–476, 2006.

[7] S. Mukherjee, S. Dey, R. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and D. K. Sanyal, “Addressing forwarder’s dilemma: a game-theoretic approach to induce cooperation in a multi-hop wireless network,” in Advances in Communication, Network, and Computing, vol. 108 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 93–98, Springer, Berlin, Germany, 2012.

[8] M. Jakobsson, J.-P. Hubaux, and L. Buttyán, “A micro-payment scheme encouraging collaboration in multi-hop cellular networks,” in Financial Cryptography: 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27–30, 2003, R. N. Wright, Ed., vol. 2742 of Lecture Notes in Computer Science, pp. 15–33, Springer, 2003.

[9] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, D. K. Sanyal, R. Neogy, and S. Pal, “A a novel incentive based scheme to contain selective forwarding in wireless sensor network,” in Computer Information Systems and Industrial Management, vol. 8104 of Lecture Notes in Computer Science, pp. 301–312, Springer, 2013.

[10] Y. M. Lu and V. W. S. Wong, “An energy-efficient multipath routing protocol for wireless sensor networks,” International Journal of Communication Systems, vol. 20, no. 7, pp. 747–766, 2007.

[11] Z. Wang, E. Bulut, and B. K. Szymanski, “Energy efficient collision aware multipath routing for wireless sensor networks,” in Proceedings of the IEEE International Conference on Communications (ICC ’09), pp. 1–5, IEEE, Dresden, Germany, June 2009.

[12] M. Ravi, B. Dezfooli, K. A. Bakar, and M. Lee, “Multipath routing in wireless sensor networks: survey and research challenges,” Sensors, vol. 12, no. 1, pp. 650–685, 2012.

[13] S. De, C. Qiao, and H. Wu, “Meshed multipath routing: an efficient strategy in sensor networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’03), pp. 1912–1917, IEEE, New Orleans, LA, USA, March 2003.

[14] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, “Protocols for self-organization of a wireless sensor network,” IEEE Personal Communications, vol. 7, no. 5, pp. 16–27, 2000.

[15] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, and D. Ganesan, “Highly-resilient, energy-efficient multipath routing in wireless sensor networks,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 5, no. 4, pp. 11–25, 2001.

[16] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed diffusion: a scalable and robust communication in wireless sensor networks,” in Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom ’99), pp. 174–185, 1999.

[17] F. Ye, G. Zhong, S. Lu, and L. Zhang, “GRAdient broadcast: a robust data delivery protocol for large scale sensor networks,” Wireless Networks, vol. 11, no. 3, pp. 285–298, 2005.

[18] R. C. Shah and J. M. Rabaey, “Energy aware routing for low energy ad hoc sensor networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’02), vol. 1, pp. 350–355, IEEE, March 2002.

[19] R. Vidyapriya and P. T. Vanathi, “Energy efficient adaptive multipath routing for wireless sensor networks,” IAENG International Journal of Computer Science, vol. 34, no. 1, 2007.

[20] X. Huang and Y. Fang, “Multi constrained QoS multipath routing in wireless sensor networks,” ACM Wireless Networks, vol. 14, no. 4, pp. 465–478, 2008.

[21] E. Stavrou and A. Pitsillides, “A survey on secure multipath routing protocols in WSNs,” Computer Networks, vol. 54, no. 13, pp. 2215–2238, 2010.

[22] R. Gibbons, Game Theory for Applied Economics, Princeton University Press, Princeton, NJ, USA, 1992.

[23] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, “A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks,” Computer Communications, vol. 35, no. 17, pp. 2125–2137, 2012.

[24] M. Nasernia and K. Tepe, “Game theoretic approach in routing protocol for wireless ad hoc networks,” Ad Hoc Networks, vol. 7, no. 3, pp. 569–578, 2009.

[25] F. Afghah, A. Razi, and A. Abedi, “Stochastic game theoretical model for packet forwarding in relay networks,” Telecommunication Systems, vol. 52, no. 4, pp. 1877–1893, 2013.

[26] S. Zhong and F. Wu, “A collusion-resistant routing scheme for noncooperative wireless ad hoc networks,” IEEE/ACM Transactions on Networking, vol. 18, no. 2, pp. 582–595, 2010.

[27] J. Liu, X. Jiang, H. Nishiyama, R. Miura, N. Kato, and N. Kadokawa, “Optimal forwarding games in mobile Ad Hoc networks with two-hop f-cast relay,” IEEE Journal on Selected Areas in Communications, vol. 30, no. 11, pp. 2169–2179, 2012.
[28] Q. Liu, J. Yin, V. C. M. Leung, and Z. Cai, “FADE: forwarding assessment based detection of collaborative grey hole attacks in WMNs,” IEEE Transactions on Wireless Communications, vol. 12, no. 10, pp. 5124–5137, 2013.

[29] D. M. Shila, Y. Cheng, and T. Anjali, “Mitigating selective forwarding attacks with a channel-aware approach in WMNs,” IEEE Transactions on Wireless Communications, vol. 9, no. 5, pp. 1661–1675, 2010.

[30] G. Zhang, K. Yang, P. Liu, and X. Feng, "Incentive mechanism for multiuser cooperative relaying in wireless Ad hoc networks: a resource-exchange based approach," Wireless Personal Communications, vol. 73, no. 3, pp. 697–715, 2013.

[31] A. Chakrabarti, V. Parekh, and A. Ruia, "A trust based routing scheme for wireless sensor networks," in Advances in Computer Science and Information Technology. Networks and Communications: Second International Conference, CCSIT 2012, Bangalore, India, January 2-4, 2012. Proceedings, Part I, vol. 84 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 159–169, Springer, Berlin, Germany, 2012.

[32] R. D. McKelvey and T. R. Palfrey, "Quantal response equilibria for normal form games," Games and Economic Behavior, vol. 10, no. 1, pp. 6–38, 1995.

[33] A. A. Pirzada and C. McDonald, "Circumventing sinkholes and wormholes in wireless sensor networks," in Proceedings of the International Conference on Wireless Ad Hoc Networks (IWWAN '05), Columbus, Ohio, USA, June 2005.

[34] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom '01), pp. 70–84, Rome, Italy, July 2001.

[35] D. Umuhooza and C. W. P. Omlin, "A metric of trust in mobile Ad hoc networks using direct source routing algorithms," in Proceedings of the Southern African Telecommunication Networks and Applications Conference (SATNAC '05), 2005.

[36] D. Sathian, R. Baskaran, and P. Dhavachelvan, "Lifetime enhancement by Cluster Head Cooperative Trustworthy Energy Efficient MIMO routing algorithm based on game theory for WSN," in Proceedings of the 3rd International Conference on Computing, Communication and Networking Technologies (ICC- CNT '12), Coimbatore, India, July 2012.

[37] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNs," IEEE Transactions on Wireless Communications, vol. 9, no. 5, pp. 1661–1675, 2010.
