CHAPTER 3

ENHANCING SECURE ROUTING USING A DYNAMIC BAYESIAN SIGNALLING GAME MODEL

3.1 INTRODUCTION

Collaboration between mobile nodes is significant in Mobile Ad-Hoc Networks. The great challenges of MANET are their vulnerabilities to various security attacks. Because of the lack of centralized administration, secure routing is a challenging task in MANET. Effective secure routing is quite essential to protect nodes from anonymous behaviours. Game theory is currently employed as a tool to analyse, formulate and solve selfishness issues in MANET.

MANET is self organized systems of nodes or installations, all cooperating to provide network functions such as routing and forwarding. Utilized in open environments, MANET is vulnerable to attack by malicious nodes, causing harm or disorder. These nodes do not reveal their identities while disrupting service. Thus, early detection is important. The network may also contain selfish nodes, installations that choose to conserve power resources rather than provide network function. Identification of selfish nodes, too, is necessary so that functional nodes do not waste resources attempting to communicate with them. Malicious node detection has previously been modeled as a Bayesian game with imperfect information. Malicious nodes attempt to avoid detection by masquerading as regular nodes, providing useful network function at an interval. This small contribution to
the network may, however, be entirely necessary in a mobile ad hoc environment with extremely limited resources and selfish nodes. Thus, exploiting the malicious node may be a viable option. Game theory can be applied to a variety of disciplines including computer networks, economics, behavioural biology and political science as well.

3.2 NEED FOR SECURE ROUTING IN MANET

The characteristics of MANET pose great challenges with respect to security design because of their dynamic network topologies, lack of centralized control and self-organizing character. Collaboration between MANET nodes is the most problematic issue for forwarding packets between nodes. Each node can forward data packets for the other nodes. This makes it difficult to design secure routing. Secure routing plays a vital role in forwarding packets in critical applications. Node mobility creates more opportunities for various security attacks in any network. Because of node mobility, cooperation between nodes is more challenging in MANET. Therefore, it is essential to develop an effective secure routing scheme to protect the nodes from anonymous behaviours.

In general, malicious nodes do not want to forward a neighbour’s packets in networks that degrade the network performance. Existing schemes are not suitable for enhancing MANET security because of routing overhead and vulnerabilities. To minimize the activities of malicious nodes, they should be monitored continuously and not be allowed to participate in routing.

Hence, it is important to protect the data in transit from the malicious nodes. Different types of security schemes have been previously developed to ensure security in MANET. However, most of the security schemes are unsuitable for MANET. The cryptography schemes used in
traditional network are not suitable for MANET due to computation and control overhead that occur during key establishment.

Various methods have been described for preventing nodes from attacks. Daojing et al 2012, proposed a Secure and Distributed Reprogramming Protocol (SDRP). It used an identity-based cryptography mechanism to enhance security for reprogramming in wireless sensor networks. It did not provide confidentiality against message interception.

Feng Li et al (2010) proposed a Game Theoretic Based Analysis (GTBA) of cooperation between regular (normal) and malicious nodes in MANET. In this approach, selfish nodes are motivated by building a reputation system. GTBA does not take multiple attacks into consideration. Game theory approaches (Mohammad et al 2012) provide effective solutions to security problems in MANET; they prevent conflict in cooperation among the mobile nodes.

Ze Li & Haiying Shen (2012), used game theoretic approaches to analyses cooperation incentives for nodes provided by reputation systems and price-based systems. They addressed the issues of enforcing cooperation among selfish nodes and discriminating malicious nodes from regular nodes. This scheme does not sufficiently address security problems such as compromised cooperative nodes.

Several works have concluded that the incentives nodes have to cooperate with their neighbours (Srinivasan et al 2005, Levente Buttyán & Jean-Pierre Hubaux (2003). These works, however, model a selfish or malicious node as never cooperative. This model is too simple and inapplicable in real world applications. Many others focus on modeling cooperation and selfishness in a network using game-theoretic approaches (Felegyhazi et al 2006, Yongkang Xiao et al 2005). In these games, nodes
decide whether to forward or not forward a packet based on a cost and benefit model. Their cost is the energy consumption necessary to forward the packet, and benefits are improved network throughput and collaboration with neighbouring nodes. In each, they show that enforcing cooperation between nodes can improve throughput, but the nodes may exhaust their power storage and retreat from the network. These works, however, do not consider the existence of malicious nodes capable of disguising their presence by providing useful network function. It is unrealistic to consider a malicious node as always attacking or a selfish node as always declining.

Hence, it is necessary to consider the unique characteristics of cooperation between nodes that should be considered in developing security protocol for MANET. The design goal of the proposed scheme is to develop secure routing. The proposed scheme uses a Dynamic Bayesian Signalling Game to analyse strategy profiles for regular and malicious nodes. It calculates the payoff to nodes for motivating the particular nodes involved in misbehaviour. Regular nodes monitor continuously to evaluate their neighbours by using the belief evaluation and belief updating systems of the Bayes rule. The proposed scheme increases the regular node’s utilities and reduces the malicious node’s utilities for involving routing operation and this is discussed in this chapter.

3.3 THE PROPOSED DYNAMIC BAYESIAN SIGNALLING GAME MODEL

The characteristics of MANET pose great challenges with respect to security design because of their dynamic network topologies, lack of centralized control and self-organizing character. Collaboration between MANET nodes is the most problematic issue for forwarding packets between nodes. The contributions of the proposed scheme are summarized as follows:
- First, it formulates a two-player Dynamic Bayesian Signalling game for the sender and the receiver.

- To find the best outcome of the strategic interaction between the sender and the receiver, three Nash equilibrium strategies are analysed: Pure Strategy with Nash Equilibrium, Mixed Strategy with Nash Equilibrium and Perfect Bayesian Equilibrium (PBE) with Bayesian Nash Equilibrium.

- Then, the payoff is to be calculated for nodes for motivating the particular nodes that are misbehaving.

- A belief update of each node is determined based on the Bayes rule in terms of action chosen, the message sent and strategy chosen, based on the probability of the node’s type.

- An algorithm is to be designed for finding belief-strategy pairs for the PBE strategy and the best response strategy for players.

The proposed SRPDBG assumes that a few nodes are not cooperating with the others and this degrades the routing performance. Anonymous behaviour of the nodes results in a packet-dropping attack. In this work, malicious behaviour of a node is determined by applying a Dynamic Bayesian Signalling Game to reveal the best actions for an individual strategy. The game is also used to achieve secure and reliable communication that results in effective cooperation among nodes. In this approach, two players, a sender (S) and a receiver (R), participate in the Dynamic Bayesian Signalling game; each player is of a type, regular or malicious. The sender chooses to send a message from a set of possible messages $M = \{m_1, m_2, m_3, \ldots, m_j\}$ based
on its own type. The receiver observes the message from the sender without knowing the type of the sender.

The receiver then chooses a feasible action from a set of actions in the space $a_i = \{\text{cooperate}(C), \text{Decline}(D)\}$. \textit{Decline} $(D)$ means that a node is not permitted to forward packets to a network neighbour, while \textit{cooperate} $(C)$ means that a node forwards packets to a neighbour. Two players receive a payoff, dependent on the type of sender. \text{PBE} is a strategy in a Dynamic Bayesian Signalling Game that assumes a scenario such as the following: the sender of type $t_j$ sends a message $m^*(t_j)$ from a set of probability distributions over $M$. $m^*(t_j)$ represents the probabilities of the node’s type $t_j$ that may take any of the messages from $M$. The receiver takes an action from the action space, either $C$ or $D$, based on observing the message and the probability distributions. In addition, the node’s strategy is determined by using the payoff calculation and a belief update mechanism. A node’s strategy may be pure or mixed or \text{PBE}. A pure strategy is one in which a node’s type should not be changed in any situation; a mixed strategy is one in which a node’s type may be changed.

The Perfect Bayesian Nash equilibrium provides a strategy profile and beliefs for each player as to the types of the other players. It maximizes the expected payoff for each player given their beliefs about the other player’s types. The \text{PBE} strategy payoff and belief update are used to determine a node’s type. A pure strategy is used to choose an action based on maximum payoff, while a mixed strategy is used to update beliefs about the other nodes. In this work, some relay nodes and sender nodes are determined to be malicious; this is reported by disseminating information to the neighbour nodes. The following algorithm chooses the optimal action for the players.
3.3.1 Algorithm

Input: Information sets of the Perfect Bayesian Nash equilibrium

Output: feasible action

**Step 1:** Specify a strategy profile for the privately informed sender and receiver node.

**Step 2:** Determine the type of node \{Regular, Malicious\}

**Step 3:** Update the uninformed sender’s and receiver’s beliefs using the Bayes rule for all information.

**Step 4:** Find the optimal response, given the uninformed sender’s and receiver’s updated beliefs

Find the feasible action \{Cooperate, Decline\}

if Not feasible action then

    Report to neighbour nodes as malicious

else

    Decide action: Decline or Cooperate

end if

In this scheme, a novel Dynamic Bayesian Signalling Game model is designed for MANET that reduces packet-drop attacks in the entire network. The sender is of type \( \Theta = \{ \text{Regular, Malicious} \} \), and the receiver believes it knows its own type with probability \( p(\Theta) = 1 \). The sender observes information about its own type and chooses an action from action space. The receiver observes the action chosen by the sender and chooses an action from
its action space. Sender \( i \)'s payoff is denoted by \( u_i(C, D, \Theta) \). The sender’s strategy is a probability distribution \( \sigma_1(.)|\Theta \) over actions \( C \) for each type \( \Theta \); the receiver’s strategy is a probability distribution \( \sigma_2(.)|a1 \) over actions \( D \) for each action \( C \). The sender’s payoff is calculated by Equation (3.1).

\[
    u_i(\sigma_1, \sigma_2, \theta) = \sum_{a_1} \sum_{a_2} \sigma_1(a_1|\theta) \sigma_2(a_2|a_1) u_i(a_1, a_2, \theta) \quad (3.1)
\]

The receiver’s payoff is calculated by Equation (3.2).

\[
    u_2(\sigma_1, \sigma_2, \theta) = \sum_{\theta} p(\theta)(\sum_{a_1} \sum_{a_2} \sigma_1(a_1|\theta) \sigma_2(a_2|a_1) u_2(a_1, a_2, \theta)) \quad (3.2)
\]

Here, \( \mu \) is the uncertainty of nodes, and \( a1 \) and \( a2 \) are the actions chosen by the sender and the receiver respectively. The PBE of this game is described by the strategy profile \( \sigma^* \) and posterior beliefs \( \mu (.|a1) \) so that

\[
    P_S : \forall \theta, u_1(\sigma_1^*, \sigma_2^*; \theta) \geq u_1(\sigma_1, \sigma_2^*; \theta) \quad (3.3)
\]

\[
    P_R : \forall a_1, u_2(\sigma_1^*, \sigma_2^*; \mu^*) \geq u_2(\sigma_1^*, \sigma_2^*; \mu^*) \quad (3.4)
\]

\[
    P_B : \mu^*(\theta|a_1) = \frac{p(\theta)\sigma_1^*(a_1|\theta)}{\sum_{\theta' \in \Theta} p(\theta')\sigma_1^*(a_1|\theta')} \quad (3.5)
\]

where \( P_S \) and \( P_R \) are the PBEs of the sender and the receiver respectively. \( P_B \) is the belief of type \( \Theta \). The receiver updates its beliefs of \( \Theta \) based on its choice of action \( D \) from type space \( \Theta \) on the posterior distribution \( \mu (.|a1) \). The mixed strategy is considered for a stranger that may be of two types \{Regular, Malicious\}. The probability of a stranger is determined as malicious if \( \varepsilon \) and its action space is \{Attack, Normal\}. The probability of \( P_S \)
is determined to be regular, and it always behaves normally. This approach is the mixed strategy for the neighbour. A node may perform two actions to a stranger: \{Doubt, Trust\}. When in doubt, it may ask for its neighbour’s help to determine the trustworthiness of the stranger, or it may request the stranger to identify itself.

3.3.2 Payoff Formulation

Payoffs define the outcomes of the players. A payoff measures the player’s outcome, called its utility. The generalized procedure for Payoff Formulation is as follows.

- If the stranger is a regular node, the target will get an amount of payoff if it trusts, where \( a > 1 \).
- If the stranger is malicious and attacks the target successfully, it will cause an amount of harm to the target.
- If the target node doubts the stranger, it will cost 1.
- If the doubt is deserved, the target node will receive amount \( b \) in a feedback message, where \( 0 < b < 1 \).
- If the trust is not valued, the target will lose amount \( b \) of payoff.
- If the stranger is a malicious node but pretends to be normal node:
  - It will cost the target more to doubt than to trust, but the doubt will induce the stranger to get a payoff of \(-1\) in the current run.
The target may threaten the stranger by doubting more frequently in a long game.

Regard the stranger as sender and the target as receiver.

Payoffs evaluate a player’s strategy. In the Dynamic Bayesian signalling game, to decline is a strategy that dominates cooperation. Strategy D of a stranger dominates C because if the target node chooses trust, then the stranger’s payoff is 3 for choosing D and 2 for choosing C. If the target node chooses doubt, then the stranger receives 1 for D and 0 for C. Hence, choosing D gives the best outcome. Similarly, the target node should choose the doubt strategy that dominates trust.

### 3.3.3 Pure Strategy with Nash Equilibrium

Nash equilibrium is a solution concept in game theory to analyse the outcome of the strategic interaction of a sender and a receiver. Each player chooses their part of the Nash equilibrium strategy, and then no player has a reason for deviating to another strategy. In the pure strategy, the players choose unique actions from a set of available actions. If the strategy is \{Attack, Doubt\} and the sender is malicious node, the best response of the receiver is to doubt. However, if the receiver doubts, the best response of sender is to behave normally. If the strategy is \{Normal, Trust\}, the sender behaves normally; then the best response of the receiver is to trust. However, if the receiver trusts, the best response of the sender is to attack.

### 3.3.4 Mixed Strategy with Nash Equilibrium

In the mixed strategy, the player chooses an action randomly from among several actions. Its choice follows a probability distribution over the set of actions from action space.
**Definition**

A mixed strategy of player $i$ is a probability distribution over its set of available actions. If player $i$ has $m$ actions available, a mixed strategy is an $m$ dimensional vector $(\alpha_1^i, \alpha_2^i, \ldots, \alpha_m^i)$ such that $\alpha_k^i \geq 0 \ \forall \ k=1,2,\ldots,m$, and $\sum \alpha_k^i = 1$.

**3.3.5 PBE with Bayesian Nash Equilibrium**

PBE is applied to refine the equilibrium generated by the perfect Bayesian Nash sub-game. It demands that subsequent play be optimal. However, it puts a player’s beliefs on the decision nodes that enable moves in non-singleton information sets that play more satisfactorily.

**Definition:**

A PBE is a strategy profile $\sigma^*$ together with a belief system $\mu$ such that

1. Strategies are optimal for every information set, given that beliefs and the opponent’s strategies are sequentially rational:
   $$\sigma_i^* (h) = \text{maximize } E_{\mu(x|h)}[\mu_i(\sigma_i, \sigma_{-i}^* \mid h, \Theta_i, \Theta_{-i})] \text{ for each information set } h \forall H_i.$$  

2. Beliefs are always updated according to the Bayes rule when applicable.

The players use a probability distribution on the action space. The strategy profile is $\sigma = (\sigma_1, -\sigma_2)$. When $\sigma$ is given, $P\sigma(x)$ is the probability that node $x$ is reached, and $h = \{x_3, x_4, x_5\}$ is the information set containing more than one node. The Belief $\mu(x)$ is specified as the probability that the player assigns to $x$, conditional on reaching $h$. The probability distribution on the
information set $h$ is calculated by using Equation (3.6), Equation (3.7) and Equation (4.8)

$$\mu (x_3) = \epsilon s$$  \hspace{1cm} (3.6)

$$\mu (x_4) = \epsilon (1 - s)$$  \hspace{1cm} (3.7)

$$\mu (x_5) = 1 - \epsilon$$  \hspace{1cm} (3.8)

The expected payoff of the receiver is calculated by Equation (4.9).

$$\mu (\sigma) = (3b - a) \epsilon s t + (a - b) \epsilon s + (a \epsilon - b \epsilon - 1) t + a (1 - \epsilon)$$  \hspace{1cm} (3.9)

The differential coefficient of $s$ is

$$\frac{\partial \mu_2}{\partial s} = (3b - a)\epsilon t + (a - b)\epsilon$$  \hspace{1cm} (3.10)

Therefore the conclusion is

when \hspace{1cm} t > \frac{a - b}{a - 3b} \hspace{1cm} \text{Equation}(3.9) > 0 \hspace{1cm} (3.11)

That is, if $s$ is increased, the payoff of the receiver will increase.

when \hspace{1cm} t > \frac{a - b}{a - 3b} \hspace{1cm} , \hspace{1cm} \text{Equation (3.9) < 0} \hspace{1cm} (3.12)

That is, if $s$ is decreased, the payoff of the receiver will decrease.

From the above solution, a threshold value is obtained that can be applied to design a secure routing protocol in MANET. If a node’s decision about another node exceeds a threshold, it will exchange decisions with its neighbours to get a more trustworthy value.
3.3.6 Payoff Calculation

In a Dynamic Bayesian Signalling Game, payoffs motivate the players who misbehave to seek the best outcome. They may be cardinal payoffs or ordinal payoffs. A payoff matrix is used for calculating the payoff. The decision maker observes the best alternative that predicts unique outcomes. Two players participate in the game: a sender and a receiver. The sender chooses an action from action space for sending a message to the receiver. The receiver observes this message and responds to it by choosing an action from its action space. The receiver has no private information if it is a single type. The receiver has some prior belief about the sender’s type. After the receiver takes an action, each player is allocated payoffs that depend on the message from the sender. The receiver takes an action and chooses a node type for responding to the sender. The expected payoff incorporates the player’s attitude towards risk. Each player receives a payoff that depends on its own action and its neighbours’ actions. The payoffs of regular and malicious nodes are listed in Table 3.1.

### Table 3.1 Payoff matrix

<table>
<thead>
<tr>
<th>Sender message</th>
<th>Node Type</th>
<th>Receiver Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal</td>
<td>Malicious</td>
</tr>
<tr>
<td>PS</td>
<td>PS</td>
<td>1, p</td>
</tr>
<tr>
<td>PS</td>
<td>SM</td>
<td>p, p</td>
</tr>
<tr>
<td>SM</td>
<td>PS</td>
<td>1-p,0</td>
</tr>
<tr>
<td>SM</td>
<td>SM</td>
<td>0,0</td>
</tr>
</tbody>
</table>

Here, $PS = \text{Prefer to send}$ and $SM = \text{Signalling Malicious}$. The expected payoff is calculated as the product of the probability of each type and the payoff of each action chosen. If the expected payoff is maximum, the corresponding actions are chosen as the sender and the receiver actions. The
sender’s expected utility is a combination of its payoffs and the actions chosen by the receiver. The sender chooses an action, either cooperate or decline, based on the receiver’s type. Because the receiver is assumed to be regular, possible actions are cooperating, decline and report. ‘Decline’ means that a node simply rejects participation, while ‘cooperate’ means that a node makes itself available for communication. The sender can conduct a simple packet-dropping attack, which is in the same form as the decline strategy of regular nodes. Sender nodes get a payoff from the attack, while regular nodes receive no gain from a decline. If a receiver chooses report, it receives a gain SM if the sender is a malicious node.

Regular nodes gains PS from a successful cooperate, where SM and PS are gains for report and cooperate respectively. Nodes could also choose Decline, which incurs zero gain and no cost even if the opponent chooses Attack. There are two Nash equilibria for PBE: \((PS, C)\) and \((SM, D)\). In \((SM, D)\), the sender does not intend to offer to forward the message and chooses to decline. Conversely, the receiver rejects the sender’s message and reports to neighbouring nodes whether the sender’s information is regular or malicious. The receiver chooses the decline action based on the PBE strategy profile. In \((PS, C)\), the sender intends to offer to forward the message to the receiver. The receiver responds to the sender’s offered message with either the cooperate or decline action. However, the receiver’s best response is to accept a message irrespective of the node type offering it. This information is not captured in the action profile \((SM, D)\) because the receiver’s information set is never reached along this path.

3.3.7 Belief-Update Process

In MANET, nodes connect and communicate directly. Malicious nodes may damage and raise the overhead in the network when they communicate with another node. To avoid this problem, a node needs to
update its belief. Bayes rule is consistent for a given strategy profile if and only if the probability is assigned by the system to every node. It is computed as the probability of the node being reached, given the strategy profile, and determines the node type. The Bayes rule is used for updating the node’s belief in terms of the action chosen, message sent, and strategy chosen based on the probability of the node’s type, as given by Equation (3.13)

\[ P(\theta|m) = P(\theta).\sigma(m|\theta)/P(\theta').\sigma(m|\theta) \]  \hspace{1cm} (3.13)

Here, \(P(\theta)\) is the probability of the node’s type, \(\sigma\) denotes the action chosen, \(m\) is the message of a sender to be sent. This allows each node to have substantiation to verify future recommendations. A node’s general behaviour can also be deduced from its past actions. This reduces uncertainty. Figure 3.1 shows the general decision process of regular and malicious nodes. Trust opinion is calculated using the Bayes rule.

A packet can be forwarded through a link only when the nodes on both sides of the link choose to cooperate. The regular node obtains feedback from its neighbour’s monitoring and evaluates the belief and sufficiency of evidence toward the opponent based on belief. It follows a threshold policy \(T\) to decide whether to report. \(T\) should be calculated as a condition that makes \(E(R) > 0\). If the threshold is reached, the regular node reports the node as malicious to all neighbour nodes. If not, the regular node chooses \(C\) with a probability \(p\) that is calculated based on its belief. Expected payoffs from each PBE strategy for the sender and the receiver are given by Equation (3.14) and Equation (3.15).

\[ E_p(S) = (1 - q)(0) + q(1), \, q \geq 0 \]  \hspace{1cm} (3.14)

\[ E_p(R) = (1 - q)(-1) + q(0), \, q - 1 \leq 0 \]  \hspace{1cm} (3.15)
Figure 3.1 describes the belief update process that determines whether a node is malicious or regular. It reports the node’s type to its neighbour, then chooses the appropriate action, either cooperate or decline.

![Diagram of belief update process](image)

**Figure 3.1 Belief-update process**

The following algorithm describes finding Belief strategy pairs for the PBE strategy and finds the best response strategies for players.

**Algorithm:**

**Input:** Incomplete Information of a Sender $S_n$ and a Receiver $R_n$.

**Output:** Belief-strategy pairs for the pure-strategy PBE.

**Main:**

Find type $t$ for $S_n$ from $\text{Type} = \{T_1, \ldots, T_L\}$ based on the distribution $p(t_n)$, where $p(t_n) > 0 \ \forall \ i$ and $\Sigma p(t_n) = 1$.

$S_n$ sends message $\text{Msg}_j$ from $M = \{\text{Msg}_1, \ldots, \text{Msg}_j\}$ based on observed $t_n$. 
R_n chooses reaction RA_k from A={RA_1, \ldots, RA_k} based on observed Msg_j.

Calculate Payoffs for sender and receiver: POS_n(t_n, Msg_j, RA_k), POR_n(t_i, m_j, a_k).

R_n has a belief \( \mu(t_n|Msg_j) \) of who sent message Msg_j, where \( \mu(t_n|Msg_j) \geq 0, \forall t_n \in \text{Type}, \Sigma t_n \in \text{Type} \mu(t_i|m_j)=1 \)

For each Msg_j \in M, RA*(Msg_j)

\[
\max_{RA_k \in A} \sum_{t_n \in \text{Type}} \mu(t_n|Msg_j) \cdot POR_n(t_i, m_j, a_k)
\]

For each t_n \in \text{Type}, Msg*(t_n)

\[
\text{Max } m_j \in M \text{ POS}_n(t_n, Msg_j, RA_k).
\]

For each Msg_j \in M, if \( \exists t_n \in \text{Type} \) such that Msg*(t_n) = Msg_j, then

R_n’s belief arises from Bayes’ Rule and S_n’s strategy.

Calculate pure strategies

\[
\mu(t_n|Msg_j) = \frac{p(t)}{\Sigma t_n \in \text{Type}} = p(t_n)
\]

Belief-strategy pairs for pure-strategy PBE

\[
[Msg*(t_n), RA*(Msg_j) \mu(t_n|Msg_j)]
\]

The proposed scheme assumes that two players are involved in a Dynamic Bayesian signalling game, sender (S) and receiver (R). Each player is a particular type \{normal, malicious\}. The sender sends a message from M based on its own type. The receiver observes the message and chooses an action from RA that may be \{cooperate, Decline\} based on its own type. The payoffs of the sender and the receiver are evaluated based on the messages, types and actions. Then, the strategy profiles of the sender and the receiver are
determined using the belief update mechanism. The belief updates of the sender and the receiver arise from the Bayes rule. The result yields the PBE strategy profile. The PBE strategy provides a feasible solution such as the types of sender and receiver, actions of sender and receiver and belief value. Furthermore, the belief value is used as threshold to perform secure routing.

Figure 3.2 Scenario of 50 nodes

Figure 3.2 shows a MANET of 50 randomly deployed nodes. The Dynamic Bayesian signalling game scheme is followed for analysing node behaviour between the sender and the receiver. A control packet is exchanged between the sender and the receiver. Node n1 discovers the malicious behaviour of nodes n4 and n2 and immediately reports it to neighbour nodes n3, n6, n7 and n8. Malicious nodes n4 and n2 are not allowed to forward the packet. An alternate routing path is selected to prevent a packet-dropping attack.
3.3.8 Find Best Response Strategy

Best outcomes of the players are found based on their beliefs, whether ordinal beliefs or cardinal beliefs. The PBE strategy provides the best response for a player when compared to strategies of other players. A sender’s best response strategy is estimated by Equation (3.16)

$$\sum a \in A \rho (a|m) u(m, a, \theta)$$ (3.16)

where \(m\) is the message, \(a\) is the action, \(\theta\) is the type, and \(\rho\) is the receiver’s behaviour strategy. A pure strategy is the best response of the sender to a receiver for a behaviour strategy. A message is specified to maximize the expected utility of a node to every type of sender. A receiver’s best response strategy is estimated by Equation (3.17)

$$V(\tilde{a}, \sigma) = \sum m \in M \sum \theta \in \Theta P(\theta) \sigma(m|\theta) v(m, \tilde{a}(m), \theta)$$ (3.17)

where \(v(m, a(m), \theta)\) is the payoff for an action chosen with a type and message; \(a\) is the action chosen, and \(\theta\) is the node’s type with a message. A receiver’s pure strategy will be the best response to the sender’s behaviour strategy if and only if it maximizes the receiver’s expected utility over all possible pure receiver strategies.

3.4 SIMULATION AND RESULTS

3.4.1 Simulation Study

This section describes the results obtained through simulation of the proposed scheme. The experimentation is performed by varying the count of malicious nodes in the MANET and three Nash equilibrium strategies are analysed: Pure Strategy with Nash Equilibrium, Mixed Strategy with Nash Equilibrium and PBE with Bayesian Nash Equilibrium.
The proposed scheme has been implemented in a network simulator (NS2). The main objective of the simulation was to enhance security in the presence of compromised nodes. The parameter settings are listed in Table 3.2. Nodes were randomly deployed in a 1000 m × 1000 m area of interest. The transmission range was 20 m. Nodes followed the Random Waypoint Model (Osama & Nigel 2013) that finds the availability of connection paths in an ad hoc network. The Dynamic Bayesian Signalling Game model analysed the effectiveness of the malicious nodes’ behaviours. The proposed scheme also evaluated the regular and malicious nodes’ strategies such as the pure, mixed, and PBE strategies. The performance of the proposed scheme was evaluated by comparing it with the related SDRP and GTBA schemes in terms of propagation delay, packet delivery ratio, routing overhead and routing latency.

The simulation results were studied by varying the network size from 50 to 200. The experiment was tested with 0 to 50 malicious nodes that may each prevent packet forwarding. SDRP and GTBA schemes are aimed to enhance security by using cryptography mechanism and reputation system respectively. The proposed scheme has integrated the PBE strategy together with a belief updating system to update a node’s belief for reducing a malicious node’s utility and increase a regular node’s utility. With the objective of comparing routing performance with related approaches, the proposed scheme has modeled a Dynamic Bayesian Signalling Game in terms of functionality for secure routing.
Table 3.2 Parameter settings for simulation (SRPDBG)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Area</td>
<td>$1000 \times 1000$ m</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>1000Sec</td>
</tr>
<tr>
<td>No of nodes</td>
<td>200</td>
</tr>
<tr>
<td>Transmission range</td>
<td>20 m</td>
</tr>
<tr>
<td>Movement model</td>
<td>Random waypoint model</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR/UDP</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Pause time</td>
<td>500 Sec</td>
</tr>
</tbody>
</table>

3.4.2 Algorithms used for Comparison

The system SDRP (Daojing et al 2012) and (Feng Li et al 2010) GTBA are taken for comparison to evaluate the performance of the proposed scheme.

SDRP is used an identity-based cryptography mechanism to enhance security for reprogramming in wireless sensor networks. It did not provide confidentiality against message interception. This scheme is more complicated due to the extra control message used in reprogramming scenario. GTBA proposed a Game Theoretic Based Analysis of cooperation between regular and malicious nodes in mobile networks. In this approach, selfish nodes are motivated by building a reputation. GTBA does not take multiple attacks into consideration. However, this scheme is unable to address malicious node’s utilities and packet dropping attack caused by a group of malicious nodes. It does not perform cooperative secure mechanism to find the malicious nodes in the network.
3.4.3 Result and Discussion

This section describes the results obtained through simulation of the proposed scheme. The experimentation is performed by varying the count of malicious nodes in a MANET, and the results obtained are analyzed. The efficiency of the proposed and related schemes is evaluated using the metrics such as propagation delay, packet delivery ratio, end-to-end delay, routing overhead, regular node’s utilities and malicious node’s utilities. Simulation results show that the proposed scheme provides effective mechanism to enhance secure routing when compared with other related schemes.

**Propagation Delay:** The propagation delay is the time required to run the code in all of the nodes in the network. It shows that the capability of the proposed scheme has less propagation delay to identification of malicious nodes.

**Utilities:** The utility is the actual average payoff to players as calculated by the expected payoff in the payoff matrix. The expected payoff incorporates a player’s attitude towards risk. The expected payoffs of a sender and a receiver are evaluated as the products of the probability of a type and the payoff of each action chosen.

**Packet Delivery Ratio:** Packet delivery ratio can be determined as ratio of the number of packets successfully delivered to the destination to the number of packets sent by the source along the path. It shows the capability of the proposed mechanism to deliver the data to the destination. This describes how efficiently the network delivers data to destination.

**Routing Overhead:** The total number of routing packets has been transmitted at time by the nodes in the network. The proposed scheme has estimated the routing overhead in the presence of malicious nodes.
Routing Latency: Routing latency is the amount of time a message takes to traverse from source to destination in a network. It shows the capability of the proposed scheme expressed as how much time it takes for a packet of data to get from source to destination.

End-to-end delay: End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

3.4.3.1 Propagation delay

Figure 3.3 shows the propagation delays of SRPDBG, GTBA and SDRP measured from the simulation. As the algorithm code size increases, the propagation delays of all schemes increase. Figure 3.3 shows that the identification of malicious nodes by SRPDBG has less propagation delay than related schemes; this is because analysis of malicious behaviour takes place between two nodes such as a sender and a receiver. Malicious behaviour is then reported to the neighbour nodes.

![Figure 3.3 Propagation Delay vs. Code Size](image)

Figure 3.3 Propagation Delay vs. Code Size
3.4.3.2 Average utility

The utility is the actual average payoff to players as calculated by the expected payoff in the payoff matrix. The expected payoff incorporates a player’s attitude towards risk. The expected payoffs of a sender and a receiver are evaluated as the products of the probability of a type from Equations (3.14 and 3.15) and the payoff of each action chosen. In any situation, at least one player is able to maximize the expected payoff through anticipating the responses to its actions. This work considered three strategies: pure, mixed and PBE. Strategies were chosen by the nodes; they provide all of the actions of the players. A pure strategy determines the action of the player in every possible situation in a game. In mixed strategies, such actions arise from a probability distribution of possible actions. A PBE is a strategy profile together with a belief system in which the strategies of every information set are optimal for its given beliefs. The utilities of nodes are determined using the strategies chosen. Comparisons of nodes’ utilities for each strategy are shown in Figures 3.4 and 3.5.

Figure 3.4 Regular nodes utilities in malicious node strategy comparison
Figure 3.4 shows that a regular node’s utility is high when it follows the PBE strategy. This is because regular nodes receive all of the opportunities to cooperate with other regular nodes and a small number of malicious nodes. However, it ensures no stimulation of the malicious nodes to attack. As shown in Figure 3.5, the utility of malicious nodes is high. When regular nodes can choose the mixed strategy or pure strategy, it reduces a malicious node’s payoff and drops their utility dramatically. The curve in Figure 3.5 shows that the utilities for malicious nodes are higher than those of regular nodes even though the regular nodes follow the PBE strategy to reduce the malicious node utilities and so improve network throughput. The PBE strategy performs better than others when malicious nodes exploit a pure or mixed strategy. Figure 3.4 shows the variation of a regular node’s belief. It is more deceptive when the malicious node exploits the mixed and pure strategy. The average utility of the malicious node is lowest because it cannot choose a route to forward packets for others. In the PBE strategy, the regular node has a chance to report the malicious type to others. Finally, the
performance analysis concludes that the PBE strategy is the best strategy for regular nodes to reduce malicious nodes’ utilities.

3.4.3.3 Packet delivery ratio in the presence of malicious nodes

In this simulation, the impacts of malicious nodes were evaluated by varying the malicious nodes in the network while measuring the PDR. Each node was assigned a trust value randomly chosen from \([0, 1]\). 10 nodes were randomly selected as source nodes to send packets to randomly chosen neighbours. If the neighbour’s trust value was lower than the threshold, it dropped the packet; otherwise it forwarded the packets. The simulation time for each test was 1000 sec. The nodes were punished only when their trust values fell below the threshold value of 0.3. They cooperated in packet forwarding when the node’s trust values fell between 0.3 and 0.7, avoiding the node being punished. If the threshold value falls below 0.3, then the node will become malicious.

The other two approaches have no effective mechanism to encourage the nodes to be cooperative. Figure 3.6 shows that 50 nodes were used in the simulation. The fraction of misbehaving nodes varied from 0 to 40%. Figure 3.6 illustrates that SRPDBG continuously maintained a higher PDR of approximately 90% when 40% of nodes misbehaved. SDRP and GTBA have a smaller PDR because they have no effective cooperative routing mechanism to detect misbehaving nodes. When the number of malicious node increases, it becomes harder to find malice-free routes from the source to destination. SRPDBG detected misbehaving nodes and performed secure packet forwarding even though the network topology was continuously changing.
3.4.3.4 Routing overhead

In this simulation, the routing overhead was evaluated for SRPDBG, SDRP and GTBA while varying the malicious nodes with different stages. Figure 3.7 shows that the routing overhead caused by SRPDBG is less than that of the other two protocols. SDRP also reduced network traffic because of its cryptographic mechanism and limited exchange of routing control messages among the nodes for the route discovery phase. On the other hand, in GTBA, the control packet flooded throughout the network until the destination was reached to find the malicious-free routing. It caused the routing overhead. In addition, when the number of malicious nodes increased, the overhead also increased because the malicious nodes did not forward the packets for others. They simply dropped the packets. SRPDBG had a minimum routing overhead of approximately 68% when 50% of the nodes were malicious because it did not allow the malicious nodes to be involved in the routing phase. Figure 3.7 shows that a malicious node drops more packets
and forwards fewer packets while keeping its trust value below threshold value.

Figure 3.7 Routing overhead Vs Malicious nodes

3.4.3.5 Routing latency

Figure 3.8 shows the routing latency for three protocols when the number of nodes varied. Routing latency is defined as the time taken to deliver packets to a destination to determine an efficient route. It was determined that the performance of the proposed scheme is more efficient than the related SDRP and GTBA schemes. It was observed that the routing latency of the proposed SRPDBG is 9 ms with 10% malicious nodes in the network and 12 ms and 13 ms for SDRP and GTBA respectively. When simulating a network with 40% malicious nodes, the time taken by the proposed SRPDBG was 28 ms. The related SDRP and GTBA schemes took more time to forward packets to their destinations. The delays in both schemes are because of link failures and more exchanges of control messages.
in the routing. SRPDBG uses the PBE strategy in the dynamic Bayesian signalling game model to find whether a node is either normal or an attacker. Only then does it allow nodes to send packets to their neighbours with minimal overhead. In this model, malicious nodes are not allowed to forward packets for others to prevent packet-dropping attacks. Therefore, it provides secure routing and enhances the performance of MANET.

Figure 3.8 Routing latency Vs Malicious nodes

3.4.3.6 End-to-end delay

Figure 3.9 shows the end-to-end delay of SRPDBG at varied number of malicious nodes as compared with SDRP and GTBA. For both SDRP and GTBA, as the malicious nodes increases, the information on a route in the routing table will quickly be out of date. Thus, both take more time to establish routes. However, SRPDBG always has a lower end-to-end delay than related schemes. One reason is the use of dynamic Bayesian signaling game to find the best outcome of the strategic interaction between the sender and the receiver in SRPDBG. The maximum delay is 0.246
seconds when 50% of nodes misbehaved, which is 30% lower than that of SDRP and GTBA. Because the related schemes do not have effective mechanism to find misbehaving nodes. Due to the more control message of routing discovery, the SDRP has a higher delay. The SRPDBG protocol achieves effective secure routing and detects the misbehaving nodes. Hence, the average delay is get decreased.

![Figure 3.9 End-to-end delay Vs Malicious nodes](image)

Table 3.3 Comparative analysis of SRPDBG with the existing schemes

<table>
<thead>
<tr>
<th>Performance Metrics</th>
<th>SDRP</th>
<th>GTBA</th>
<th>SRPDBG Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagation Delay (sec)</td>
<td>272</td>
<td>281</td>
<td>235</td>
</tr>
<tr>
<td>Regular node’s Utilities (%)</td>
<td>92.56</td>
<td>93.67</td>
<td>95.56</td>
</tr>
<tr>
<td>Malicious node’s Utilities (%)</td>
<td>21.6</td>
<td>1.68</td>
<td>1.2</td>
</tr>
<tr>
<td>Packet Delivery Ratio (kb/sec)</td>
<td>84.7</td>
<td>86.80</td>
<td>90.2</td>
</tr>
<tr>
<td>Routing Overhead (%)</td>
<td>74.08</td>
<td>78.78</td>
<td>68.57</td>
</tr>
<tr>
<td>Routing Latency (msec)</td>
<td>45</td>
<td>46</td>
<td>27</td>
</tr>
<tr>
<td>End-to-End Delay(sec)</td>
<td>0.71</td>
<td>0.626</td>
<td>0.246</td>
</tr>
</tbody>
</table>
Table 3.3 shows the comparison of SRBDBG with the existing system for different parameters. The parameters may be the propagation delay, packet delivery ratio, regular node’s utilities, malicious node’s utilities, routing overhead, end-to-end delay and routing latency. The reliability of routed packets can be achieved through the proposed secure routing scheme. The proposed scheme resists the malicious activities through dynamic Bayesian signalling game model and is capable of achieving high packet delivery ratio with less routing overhead.

In this analysis, SRPDBG has a better packet delivery ratio (90%), less end-to-end delay (0.246 sec) and less propagation delay (235 sec) than the other two protocols. SRPDBG causes minimal routing overhead compared to SDRP and GTBA because the proposed scheme prevents routing in the presence of malicious nodes.

3.5 SUMMARY OF THE CONTRIBUTION

The proposed scheme has used a Dynamic Bayesian Signalling Game model to reveal the best actions of individual strategy to minimize the utilities of malicious nodes in MANET. If a node is malicious, it cooperates less and may degrade MANET performance. A novel scheme of payoff formulation is developed for senders and receivers. Payoffs are used to motivate the misbehaving players. Each player is allocated payoffs that depend on its actions and its neighbours’ actions. A receiver takes an action and a node type for responding to the sender.

It used a belief-updating system to update a node’s belief in terms of action chosen, message sent, and strategy chosen. A regular node in the network periodically follows the belief-update process for its private information; it then chooses a probability to cooperate with its neighbouring node. A packet can be forwarded through a path when the nodes choose to
cooperate, preventing a packet-dropping attack. This is a novel way to enhance secure routing and motivate effective cooperation among nodes. A regular node obtains feedback from neighbour monitoring and evaluates its belief. It follows a PBE decision rule to report its node type to neighbours. This game model also analysed the equilibrium strategy profiles for senders and receivers based on its payoffs and belief updates. It emphasizes reducing a malicious node’s utility and increases a regular node’s utility when it follows the PBE strategy.

Simulation results show that the PBE strategies for senders and receivers are better than pure or mixed strategies. Therefore, it can be concluded that increasing the number of monitoring nodes improves the network performance as a whole.