CHAPTER 5

GAME THEORY AND DEMPSTER SHAFER THEORY-BASED SECURE RPL OVER IOT

This chapter proposed a DODAG specific trust-based RPL security solution named as S-MODEST. For enhancing the routing efficiency with successful attack detection, the S-MODEST employs a context-aware non-cooperative game model and Dempster Shafer theory. Finally, the effectiveness of S-MODEST is compared with SecTrust and evaluated for diverse network scenarios.

5.1 Impact of Malicious dropping attacks in RPL

Even though the design of cryptographic systems in RPL routing protects the network from external attacks, the presence of internal attackers compromises the cryptography based security mechanism and thereby launching severe attacks that cause network degradation. One of the serious internal threats in RPL routing is packet dropping attacks that cause global impact due to the packet forwarding nature of an RPL network. Initially, malicious dropping attackers gain access to the network and drop data packets that are forwarded to them. For detecting these attacks, the existing mechanisms designed routing behavior-based detection methodologies for handling malicious activities. However, the possibility of these malicious nodes overhearing the network activities and posing as nodes that suffer from collision dropping is high. For instance, the dropping attacks act as normal nodes in the route discovery by purposely announcing a small rank value. Under such a situation, a malicious node appears to be legitimate, and dropping only certain data packets leads to the malicious dropping attackers misclassified as collision dropping. Hence there is a necessity of precisely classifying the malicious misbehavior nodes from the misbehavior due to network constraints.

5.1.1 Role of Game theory Model in RPL Security

Conventionally, the Game Theory model plays a significant role in solving false positive issues during attack detection in IoT networks. The Game Theory offers a set of modeling tools where the interactions of nodes are considered as a game with the inclusion of efficient monitoring strategies for the IoT environment. The advantage of game theory platforms is that they study situations of conflict and cooperation and thereby solving conflicting interests through an analysis of interactive decision-making problems. The Game Theory model is categorized as cooperative, and non-cooperatives based on interdependence between players. The non-cooperative game theory provides a detailed model of all the interactions available to the players. Cooperative game theory model represents all possible results of players in different combinations. However, the non-cooperative game theory exhibits self-enforcing agreements that help in securing IoT communication effectively. Also, the evolutionary game model is applied in the IoT environment for information diffusion and router selection processes.

5.2 Game Model Formulation of S-MODEST

Initially, the IoT network is modeled as a non-cooperative game. This model contains a set of sensors as players (N), a strategy space (S), and a utility function (F). Thus, the network G can be denoted as G = {N, S, F}.

Players and Game: The game among the players is represented as a graph G (N, E), where E refers to the direct connection between the players $E \subseteq N \times N$. For constructing IoT, N number battery-limited tiny devices N is crucial. Such tiny devices can able to establish wireless communication and forwards the sensed information to one of the border nodes that are connected to the IPV6. The devices are named as Gateways (N_G). The S-MODEST models interactions between the devices as a non-zero sum game in G. The primary elements of the non-zero sum game model for IoT environment are demonstrated in table 5.1.

Table 5.1: Elements of the Game model of IoT Environment

Non-Zero Sum Game Model	IoT Environment
Players	Nodes

Strategy	Cooperate and non-Cooperate
Utility Function	**1)** Direct Trust and Indirect Trust **2)** Context certainty level (packet drop due to collision)

The primary focus of the evolutionary game is to choose a more energetic and trusted router device. In a network G with N number of players, the F can be represented by a two-tuple, i.e., F($HW_{trust,\ energy}$, $LW_{trust,\ energy}$). The non-zero sum game model returns the utility value of players. The tuples denote the player sets possess high weighted players and those with less weight. The weight denotes the moderated weight between the trust value and energy of a player.

$$\mathbf{N} = \mathbf{HW_{trust,energy}} \cup \mathbf{LW_{trust,energy}} \;\&\&\; \mathbf{HW_{trust,energy}} \cap \mathbf{LW_{trust,energy}} = \emptyset$$

It means that every player in N belongs to either $\mathbf{HW_{trust,energy}}$ **or** $\mathbf{LW_{trust,energy}}$.

Table 5.2: Elements of the Game model of IoT Environment

Evolutionary Game Model	DODAG Structure
Players	Nodes $\mathbf{HW_{trust,energy}}$ **and** $\mathbf{LW_{trust,energy}}$
Strategy	Parent and Child
Utility Function	Weighted trust and energy of a node

Each individual in N has two strategies to act to be a parent player or child player. The utility values are computed using the evolutionary game model. Table 5.2 describes the elements of the evolutionary game model in an IoT environment.

Hostile Environment: Due to the nature of the wireless medium, the IoT devices N are susceptible to routing attacks. Considering that the network G comprises the number of intentional droppers M in an environment, where the terms M_M and M_S denote the number of malicious and selfish nodes Є M respectively. The selfish device is not cooperative, whereas a malicious device intends to repair the network activities. Unlike selfish nodes, the malicious droppers drop the packets to harm the device resources. Due to the hostile environments of connected tiny sensor devices, the routing enforcement for converting the selfish players to become benevolent is a cornerstone of IoT.

Utility Function: The utility function offers a payoff, which refers to a specific outcome of the strategy that is chosen by a player across the network. The primary intention of all the players in a non-cooperative game model is to maximize the utility function of the strategy of another player. In the same way, each selfish player is motivated to act as a router for forwarding other packets. Also, each player (i) chooses its strategy S_i from the strategy space S. The strategy space is defined by S = {cooperate (C), non-cooperate (NC)}, where C represents a packet forwarding, and NC represents the packet dropping occurrence either due to collision or intentional dropping (selfish or malicious activities). Thus, the context-dependent trust calculation in S-MODEST differentiates the dropping due to selfish or malicious. Furthermore, the utility function in S-MODEST motivates the selfish players for better cooperation in routing. Thus, the S-MODEST can reduce the impact of malicious players that always choose the non-cooperative strategy and offer high security in IoT routing.

5.3 Overview of the S-MODEST

The S-MODEST attempts to extend the fundamental RPL routing protocol that adopts the routing behavior observation to cope with the malicious activities and relies on a context certainty level for formulating the parent selection as a coalition formation. The extended protocol named S-MODEST incorporates three components are Building routing behavior trust on Non-zero sum Game Model, Emphasizing Strength and Light-Weight Defense System, and Coalition Formation using the evolutionary game model.

Constructing routing behavior-based trust with Non-Zero Sum Game Model: To build the non-zero sum game model, the S-MODEST considers the context attributes as prime attributes in mixed strategies (C & NC). However, if the players follow a pure strategy (C & C), the context information such as packet drop probability due to collision is an insufficient factor, as the players already have been providing perfect cooperation without losing more packets. Thus, the S-MODEST builds the DODAG-specific context information only upon the mixed strategy model. This procedure increases the feasibility of implementing a lightweight security scheme on IoT without degrading the trusted accuracy.

Emphasizing Strength and Light-Weight Defense System: Although the trust measurement based on direct observation is considered as the interactions between players, the S-MODEST may tend to incorporate the players in the pure/mixed strategies incorrectly. To develop a new definition of a game strategy to influence the trust formation in the IoT, the S-MODEST takes into account the certainty level in trust computation. The certainty represents the number of interactions involved in trust measurement. The indirect trust derivation is considered only for less interactive players. This procedure balances the trust accuracy and overhead cost for trust measurement.

Coalition Formation using Context certainty behavior-based final trust: The number of child nodes connected with a single parent node in DODAG structure is utilized as proper collision evidence, and it assists the non-zero sum game model to differentiate the malicious activities from collision dropping in mixed strategy. However, the malicious node with the lowest rank acts as a parent for an additional number of nodes as per the RPL routing nature. It turns the S-MODEST unfit to differentiate the collision scenarios from adversary scenarios. The evolutionary game model considers the RPL-specific factor such as a high - rank variance to observe the packet dropping at non-cooperative parent player and confirms it as malicious dropping since the DODAG structure allows several children to connect with a parent node. Hence, it is vital to exploit the rank variance among the players to avoid misclassification of the malicious nodes dropping as collision dropping, and neglecting the impact of inaccurate packet dropping detection on IoT routing efficiency.

5.3.1 Building routing behavior trust on Non-Zero Sum Game Model

The non-zero sum game model based fully distributed trust calculation of S-MODEST necessitates that each player observes the co-player in different perspectives from routing cooperation to a certain level. The generic trust model regardless of the DODAG structure is not compatible with IoT environments. Thus, the non-zero sum game model extracts the number of connected children under a parent node from the DODAG structure and differentiates the collision data loss from malicious activities. The trust measurement of S-MODEST taking into account both direct routing interactions and indirect trust offered by adjacent devices. In the quantification of trust, it reflects the expectation of a player that a specific co-player can cooperate in the future with the probability estimated in the past. Based on this rationale, the probability of a successful forwarding rate is the measure and that wise to calculate the trustworthiness. The derivation of indirect trust is beneficial only for minimum interactive players. The players exchanging a fewer number of interactions reduce the confidence level of direct observation of successful forwarding probability. Thus, the S-MODEST performs the indirect trust measurement using Dempster-Shaffer theory to maximize the trust precision in IoT. To transform the generic trust value into the contextual trust information, the non zero sum game model applies the DODAG-specific rank variance factor in trust computation.

Direct Trust Measurement: To accomplish the low-cost implementation of the defense system, most of the conventional works employ simple equations to evaluate direct trust. The Direct Trust metric (DT) is associated with Successful (SI) and Failed Interactions (FI). Based on the S-MODEST, each node i estimates the trust value DT on node j (denoted as $DT_{(i,j)}$) using the following equation:

$$\mathrm{DT}_{(i,j)} = {}^{\mathrm{SI}_{(i,j)}}\!\big/_{\mathrm{SI}_{(i,j)} + \mathrm{FI}_{(i,j)}} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \ldots.\,.\,(5.1)$$

Generally, the direct trust observation is enough to conclude the routing behavior of a node. However, it requires an abundant number of straight interactions among the communicating devices, resulting in high complexity. For the newly elected parent nodes, it is insufficient to measure the direct trust with limited interactions. Although incorporating indirect trust computation is a benefit for observing the behavior of newly elected parent nodes, the consideration of a sufficient number of interactions is necessary for the direct trust measurement. The S-MODEST employs the certainty factor {1-(Int)$^{-1}$}, which denotes the confidence level of the direct trust type, concerning the number of interactions. The observation of direct trust becomes trustworthy when many numbers of interactions are required. Even though the generic trust model, regardless of context is not compatible with the DODAG scenarios. Notably, it is not only the malicious behavior that disrupts the routing process in IoT, but also the collision. The parent node with many children may likely drop the packets due to collision and degrade the performance of the routing process. Thus, the remaining certainty factor 1-{1-(Int)$^{-1}$}also takes into account the number of Connected Members (CM) to the same parent node and appends the probability of packet dropping due to collision during trust measurement. Indirect trust calculation through the trust exchange can be beneficial for newly activated or less interactive players more than others. Although frequent message exchange to the reputation system improves the certainty of trust measure, it is not appropriate to the resource-limited IoT players. Thus, the non-zero sum game model justifiably applies the restricted Dempster-Shaffer theory in trust appraisal.

$$\mathrm{C} - \mathrm{DT}_{(\mathrm{i,j})} = \left\{1 - \{1 - (\mathrm{Int})^{-1}\}\left\{\mathrm{DT}_{(\mathrm{i,j})}\right\}\right\} * \left\{1 - \{(\mathrm{CM})^{-1}\} * \left\{\mathrm{DT}_{(\mathrm{i,j})}\right\}\right\} + \{1 - (\mathrm{Int})^{-1}\}\left\{\mathrm{DT}_{(\mathrm{i,j})}\right\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. . \ldots (5.2)$$

Dempster-Shaffer Theory-Based Restricted Evidence Collection: To prevail the indirect trust value, each player offers a reputation request packet when the number of direct interactions with the co-player is minimum. If all the neighboring nodes in the communication range involve in the provision of reputation response, the network is highly burdened, and the routing efficiency tends to decline. The common one-hop neighbors between the players act as evidence providers in the network. To diminish the routing overhead considerably, the S-MODEST limits the number of evidence providers precisely. Typically, random selection is applied to limit the number of reputation responses. However, it is not always appropriate in an untrustworthy environment. Moreover, receiving a reputation response from different nodes with the same opinion does not contribute to improving the accuracy of trust measurement. Thus, S-MODEST utilizes the MAC layer packet broadcasting capability in restricting the reception of reputation response from the neighbors having the same opinion on a co-player.

The restricted evidence collection method of S-MODEST offers priority to reputation response evidence providers, based on their direct trust. The sender initiates to broadcast the reputation request message with the ID of selected evidence providers in the order of priority. The best forwarder node broadcasts the reputation response message with its trust value of an observed player, and other forwarding candidates receive the reputation response message of the maximum priority node. If its own opinion on the same observed player is similar to the received message, it does not broadcast the reputation response message in a time slot. In S-MODEST, when the trust value of an observed node is similar to the higher priority node the evidence response of a higher priority player suppresses the next priority node. Otherwise, the next priority evidence provider broadcasts its trust in observing the player at its scheduled time. To maintain the trust accuracy, the sender node accepts the response of higher priority node in n+1 time, where n represents the subsequent evidence providers that obey the opinion of higher priority node without responding to the reputation message.

The player obtains a sufficient level of trust to execute the Dempster - Shaffer theory using a restricted evidence collection model of S-MODEST. Considering a scenario, where the player A interacts with S. The trust of node A (C-DT$_{(A, S)}$) denotes that the node S is being suspected. The node A broadcasts the reputation request message for node S at t time. The common neighboring nodes of node A and S is node B, C, and D. Node B and C claim about node S that it is a suspected one, but node D claims the node S as a legitimate node. The S-MODEST calculates the belief of a Hypothesis H and H^, where H denotes that a node S is suspected and H^ represents “not H”. The belief of neighboring nodes B and C on H (Bel(H)) and the belief of node D on H^ (Bel(H^)) are estimated as follows.

$$\mathrm{Bel(H) = AVG\ m(H_i)}$$
$$\mathrm{H_i \subset H} \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5.3)$$
$$\mathrm{Bel(H\hat{}) = AVG\ m\big(H_j\big)}$$
$$\mathrm{H_j \subset H} \qquad\qquad \ldots\ldots\ldots\ldots (5.4)$$

In the equations (5.3) and (5.4), i and j denote a set of nodes that provides evidence as true for H and H^, respectively. The plausibility function offers weight to the evidence that does not refute H.

$$\mathrm{Pls(H) = 1 - \left\{\prod 1 - \big(C - DT_{(A,i)}\big)\right\}}$$
$$\mathrm{H_i \subset H} \qquad\qquad \ldots\ldots\ldots\ldots (5.5)$$

The S-MODEST takes both the belief and plausibility values of H to estimate the total Indirect trust on H, ID(H).

$$\mathrm{ID(H) = {(Bel(H) * pls(H))}\Big/{(1 - Bel^{\wedge}(H) * Bel\hat{}(H\hat{}))}} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots (5.6)$$

The average value of (C-DT$_{(A, S)}$) and ID(H) denotes the Total trust (TT) on node S. According to the total trust value, the S-MODEST neglecting the malicious players that always choose a non-cooperate strategy of game model, resulting in high security in IoT routing.

5.3.2 Utility for Different Strategies and Nash Equilibrium

The Nash Equilibrium (NE) is reached, when the players select equitable strategies or when no player has anything to gain by changing only its strategy. Even though the (NC, NC) strategy profile is fair, but it is not the NE since it is undesirable from the network context. The reward for a player that selects to cooperate in routing is denoted by (V-e), and for a player that selects not to cooperate is denoted by (V), only when a co-player chooses a cooperation strategy. In case both the players choose not to cooperate, the punishment that each player receives is by (−r).

Table 5.3: Utility in a Non-Zero Sum Game Model

Player 1 Strategy	Player 2 Strategy			
	C		NC	
	Strategy	Utility (F-TT)	Strategy	Utility (F-TT)
C	{(V-e), (V-e)}	=TT	{(V-e), (V)}	≥TT
NC	{(V), (V-e)}	≥TT	{(-r), (-r)}	=TT

Consider that $V > (V - e) > -r$ and the optimal equilibrium strategy profile is $(V - e, V - e)$. However, this situation cannot be realized in all games due to the malicious behavior of some players. Notably, the S-MODEST employs the trust value as a utility and selects a secure parent coalition. The players may select the same (pure) or different (mixed) strategies. The S-MODEST uses the utility or trust as evidence to identify the strategies of players. The trust of pure strategy (C, C) is always higher than the mixed strategy. If every player prefers to cooperate, the pure strategy of all the players is a Nash equilibrium. To have a perfect NE using accurate trust evaluation, the S-MODEST maximizes the trust value with the probability of collision impact on packet forwarding. However, differentiating the collision dropping from malicious behavior for the number of connected members is not always accurate. In such a case, the estimated C-DT makes the TT value of mixed strategy players to denote as a pure strategy due to the addition of packet drop probability by the data collision, as shown in equation (5.2). Due to this problem, the TT value tends to be higher than the original trust value, which is denoted as F-TT. For each strategy, the final trust value, F-TT of a node is represented in Table 5.3. Mostly, the dropping attackers attract other nodes by setting the lowest rank in DIO message broadcasting. The node may advertise the first rank or maliciously change the rank to become low. According to the nature of RPL routing, the victims may request the malicious node to be preferred as the parent. The parent node drops the forwarding packets intentionally; however, it may be misclassified as collision dropping. In this manner, the mixed strategy of the players is denoted as a pure strategy. The consideration of collision impact renders the S-MODEST to denote the malicious scenario as a Nash equilibrium. There is a need for estimating the TT value closer to the original trust value, F-TT. To correctly identify the Nash Equilibrium state, it is essential to reach a more reliable conclusion of whether the misbehavior is a result of malicious activity or due to the collision of the parent node. Both the malicious node behavior and the collision dropping are equally treated as malicious in the existing detection techniques. Hence, incorporating a general context-aware trust model in the non-zero sum game is not combative with dropping attacks. Thus, the S-MODEST uses DIO-message information to extend the context-dependent trust estimation to differentiate the pure strategy from mixed strategy players accurately.

5.4 Malicious Attack Detection by using RPL-Specific Contextual Trust Measurement

The primary purpose of this component is to exploit the advantage of RPL-specific information to extend the context-aware utility function in the identification of pure and mixed strategies precisely. In most dropping misbehavior, nodes cooperate during the DODAG building process with a minimum rank; however, they refuse to transmit the data packets during the data forwarding phase. The proposed S-MODEST scheme utilizes the RPL-specific certainty measurement based on the rank variance to detect such type of misbehaving nodes in the network. High-Rank Variance (RV) results in a reduced certainty level, and the combination of more low direct trust value and certainty level confirms that the node dropping is intentional due to the malicious behavior, and not because of the collision. The final direct trust value is estimated using the following equation.

$$\mathrm{F} - \mathrm{TT}_{(\mathrm{i,j})} = \begin{cases} \mathrm{TT}_{(\mathrm{i,j})} * (1 - \mathrm{RV}) & \text{if RV} > 1 \\ \mathrm{TT}_{(\mathrm{i,j})} & \text{otherwise} \end{cases} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots(5.7)$$

$$\mathrm{RV} = \left\{\left[\sum_{\mathrm{i=1}}^{|\mathrm{Ne}|} \mathrm{R_i} \Big/ |\mathrm{N_e}|\right] - \left\{\mathrm{N} * {}^{(3.14 * \mathrm{Tr}^2)}\Big/_{\mathrm{HW}}\right\} \Big/ \mathrm{R}\right\} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5.8)$$

The term (3.14*T_r^2) refers to the communication area of a node. Even in the case of a sparse environment, the rank variance is likely to be in the range between 0 and AVG R - {N*(3.14*T_r^2)/(HW)}/R}. Increasing the limit of RV up to less than 1 denotes a high level of trustworthiness of a node. Otherwise, the player is an attacker. Integrating the rank variance in TT using the equation (5.7) is the final trust for nodes in IoT. Notably, the TT is equal to the F-TT value of the pure strategy players as well as the mixed strategy players with less than 1 RV. The minimum trustworthiness of a player significantly diminishes the probability of getting selected as a parent, and those players categorized into the pure strategy may be selfish or intentional droppers. Thus, the S-MODEST manages to classify those players into the mixed strategy. The mixed strategy players may drop the packets due to selfish or malicious behavior. To enforce the routing cooperation of selfish nodes, the S-MODEST receives the non-cooperative co-player in the mixed strategy as a suspected node and confirms its nature of behavior with the non-zero sum game model.

5.4.1 Trusted DODAG Formation using Evolutionary Game Model

The evolutionary game model builds a perfect DODAG scenario, where the co-player or the parent player in the mixed strategy is self-enforced to cooperate with a suspected node for a while. To enforce the trusted DODAG formation, the evolutionary game model plans to establish the rules to restrict the parent selection process in RPL routing. This game model regulates the players with weighted trust and energy value in selecting the parent node and building the DODAG structure. Unlike the malicious nodes, the selfish nodes do not keep the same strategy entirely. The selfish nodes follow the strategies of (NC, C) or (C, NC), but after some time, the strategy of (NC, C) or (C, NC) tends to (NC, NC). However, selfish nodes do not want their strategies to get affected. The malicious nodes still follow the same strategy of NC. Thus, the evolutionary game model avoids malicious players from the DODAG formation. To encourage the nodes in the selfish mode, the packets from them are not forwarded by the legitimate players in the network. To do it, the trusted DODAG creation is paramount. To encourage the players in $\mathrm{HW_{trust,energy}}$ to be the parent player and meanwhile prevent the players from $\mathrm{LW_{trust,energy}}$ from being selected as a parent player, the evolutionary game model devises the utility function. The evolutionary game model involves two kinds of players concerning the weighted trust and current energy factor.

$$\mathrm{W_{trust,energy(i)}} = \mathrm{F} - \mathrm{TT} * {}^{\mathrm{Current\ Energy_{(i)}}}\!/_{\mathrm{Initial\ Energy(i)}} \quad \ldots\ldots\ldots\ldots\ldots (5.9)$$

When the nodes have $\mathrm{W_{trust,energy(i)}}$ less than 0.5, it is categorized into $\mathrm{LW_{trust,energy}}$, otherwise, it is grouped under the class of $\mathrm{HW_{trust,energy}}$. The utility of the evolutionary game model is shown in table 5.4. Where Δ, E, and Ƙ represent energy difference between the players of two classes, energy consumed by a player, when it acts as a parent, and the ratio of successful interactions respectively. The negative Ƙ term represents the ratio of failure interactions of a parent player, due to either the malicious activity or weak battery.

Table 5.4: Utility in an Evolutionary Game Model

Player 1 ∈ $\mathbf{HW_{trust,energy}}$	Player 2 ∈ $\mathbf{LW_{trust,energy}}$			
	Parent		Child	
	Strategy	Utility (F-TT)	Strategy	Utility (F-TT)
Parent	{(Δ-E), (Δ-E)}	F-TT	{(Δ -E), (Δ)}	(F-TT + Ƙ)/2
Child	{(Δ), (Δ-2E)}	(F-TT +(- Ƙ))/2	{(Δ), (Δ)}	Ƙ

When both the players have the same strategy, such as a parent, there is no change in the F-TT value since such a scenario tends to both packet loss and successful transmissions. Only when the player ∈ $\mathbf{HW}_{\mathbf{trust,energy}}$ is selected as a parent; the final trust value increases. In another case, the packet drop is caused either due to malicious activity or poor resources. Thus, it reduces the final trust value of the utility function. If no parent player in the IoT environment, there is no change in the energy difference between the players of various classes. Since there is no interaction between the players over time and so the value of Ϗ is assigned as zero. When the node from the $\mathbf{HW}_{\mathbf{trust,energy}}$ class is acting as a parent the network performance improves significantly. In accordance with the utility function of the evolutionary game model, the S-MODEST exploits $\mathbf{W}_{\mathbf{trust,energy}}$ from equation (5.9).

The S-MODEST uses the entire path weight as a metric to construct routing tables without creating loops by extending the utilization of trust in parent selection or coalition formation, the, in addition to the individual trust and rank metric used by RPL. The S-MODEST protocol extends the DIO message broadcast to include the "multiplicative route weight" field. Then, the sender node selects a path with the highest weight as a parent, resulting in improved certainty in packet delivery not only in a single hop but throughout up-to N_G. To punish the attackers, the packets from a node with trustworthiness below the threshold are not allowed to forward by other nodes. This punishment threshold is decided based on the packet drop due to the collision. Using non-cooperative game models and context-aware trust model, the proposed S-MODEST improves security as well as routing performance over the IoT environment.

5.5 Performance Evaluation of S-MODEST

The proposed S-MODET employs the Cooja simulator of the Contiki operating system to analyze its performance effectiveness. This section describes the comparative simulation results of S-MODEST with an existing SecTrust protocol (Saled et al., 2013). In Cooja, the emulated Tmote Sky is used in configuring the IoT devices. Each node sends the readings to the Gateway node periodically. This traffic information is recorded for 60 simulation seconds. The S-

MODEST is simulated in the area of 100 X 100m^2 in which 31 and 61 nodes are randomly deployed. It simulates the Contiki MAC with a node range of 50m. A bandwidth of a node in the network is 2 Mbps. CBR generates the data in 10 Sec with the size of 127 bytes, and UDP configures the transport layer. The propagation model used is a TwoRayGround model. To analyze the effect of the malicious nodes in the IoT environment, this work conducts simulations with a varying number of attackers. Moreover, this work analyzes the effect of the network area on the performance of S-MODEST and SecTrust. The network area is varied from 100 to 300m^2. Further, the data traffic impact on routing performance is also analyzed by varying the data transmission interval from 10 to 30 seconds.

5.5.1 Performance Metrics of S-MODEST: Performance comparison of S-MODEST with conventional SecTrust is performed using the following metrics.

Throughput: The rate of delivered packets to the gateway node.
Normalized Overhead: It is the ratio of the number of control packets involved in the transmission of data packets.
Energy Consumption: It is the amount of joules consumed to deliver the data from source to destination.
Detection Accuracy: It is the ratio of correctly identified attackers to the total number of attackers.
Routing Enforcement: It is defined as the rate of change in selfish forwarding behavior.

5.5.2 Simulation Results of S-MODEST

For effective analysis of S-MODEST over diverse scenarios, the simulation results are obtained varying the network area from 100 to 300m^2 in the network.. The consideration of non-cooperative game models with the contextual trust measurement has improved the detection accuracy in S-MODEST. Beyond the point of 150m^2 of the network area, the detection accuracy of S-MODEST starts to degrade. An increase of more than 150m^2 of network area extends the distance between the nodes and decreases the availability of nodes in the class of $\mathbf{HW_{trust,energy}}$. This scenario leads to the observation failure of some data interactions. Beyond 150m^2 of network area, the detection accuracy of S-MODEST declines from 100% to 57.2%, but it performs better in comparison with SecTrust.

Performance Analysis by Varying Network Area: Figure 5.1 demonstrates that when the network area is small, the detection accuracy of S-MODEST with 30 and 60 nodes topology is relatively close to one another when compared with the case of a large area. The observed influence of the network area on the detection accuracy of the S-MODEST is reasonable, in contrast to the existing SecTrust. The S-MODEST takes into account the DODAG and RPL specific features and reduces the false positive rate using non-zero and evolutionary game models. For instance, with the small network area, both the S-MODEST and SecTrust attains nearly 95% and 37.5% of detection accuracy respectively. However, the difference in detection accuracy between the algorithms increases with the network area.

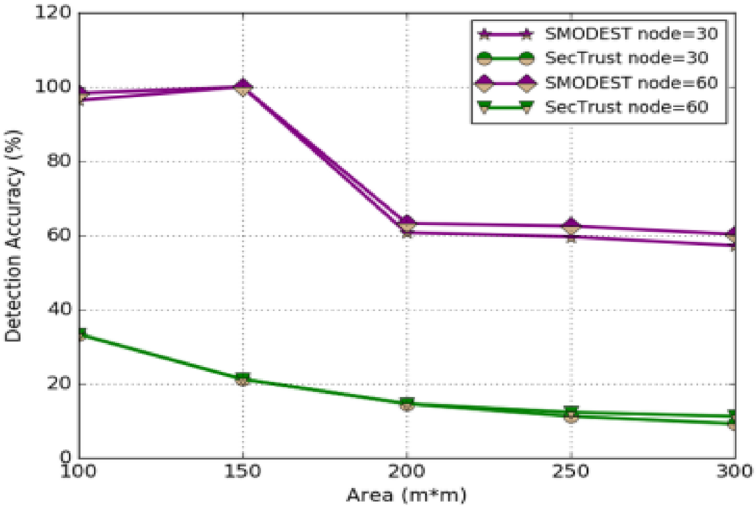

Figure 5.1: Performance Evaluation of S-MODEST by Varying the Network Area in terms of Detection Accuracy

From figure 5.2, it is observed that the throughput of S-MODEST has always been comparatively better than that of the existing SecTrust. The number of IoT nodes is directly proportional to the network load, as every node transmits the sensed information to the gateway node periodically. The S-MODEST involves the most trustworthy and highly energetic path in delivering the data packets to the gateway using non-zero sum, and evolutionary game models to improve the rate of packet delivery. However, the SecTrust assumes that all the trust evidence provided by the neighboring nodes are always trustworthy, which is not perfect to consider in the case of intelligent malicious activities. The performance of S-MODEST improves the throughput by 39.7% more than that of SecTrust with 60 numbers of node topology over 300m^2 of the network area.

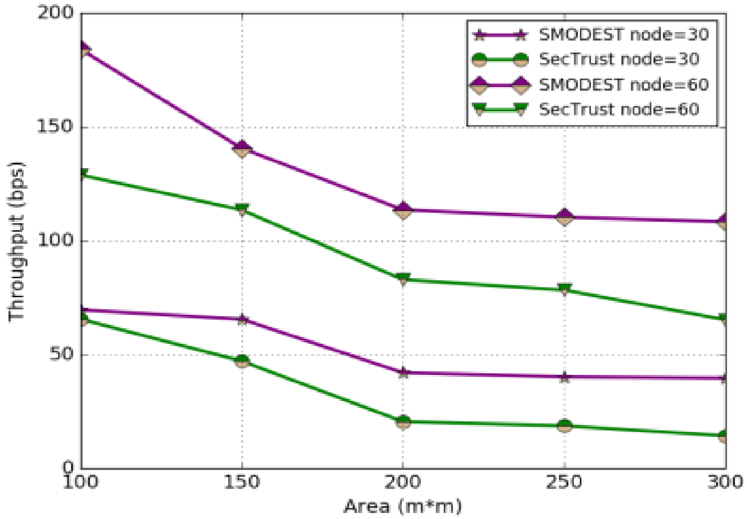

Figure 5.2: Performance Evaluation of S-MODEST by Varying the Network Area in terms of Throughput

The normalized overhead of the SecTrust is high compared to the S-MODEST as shown in Figure 5.3. If the number of neighboring nodes increases in a communication range, the normalized overhead of the systems builds up linearly. Though S-MODEST involves several processes for selection of secure routing path to the gateway node, the normalized overhead of S-MODEST is reasonable, due to the compensation of routing overhead through the restricted Dempster-Shaffer theory. However, the SecTrust collects the trust evidence from all the one-hop neighbors periodically and hence carries high routing overhead, compared to S-MODEST. In 30 node topology, the S-MODEST increases energy consumption by 66% than 60 node topology as shown in Figure 5.4.

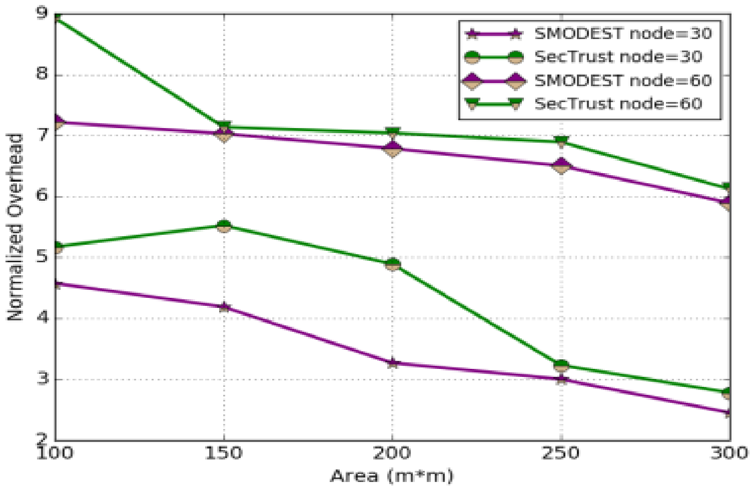

Figure 5.3: Performance Evaluation of S-MODEST by Varying the Network Area in terms of Normalized Overhead

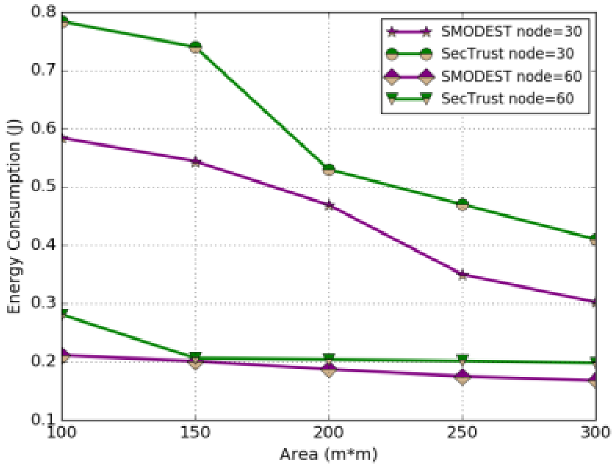

Figure 5.4: Performance Evaluation of S-MODEST by Varying the Network Area in terms of energy consumption

Performance Analysis by Varying Attackers: Figure 5.5, Figure 5.6, Figure 5.7, and Figure 5.8 demonstrates the performance of S-MODEST and SecTrust over a different number of nodes and attackers. The detection accuracy in Figure 5.5 represents the correctness of the trust model in detecting the malicious nodes. The detection accuracy of the proposed work is higher, as it identifies the malicious nodes using the non-zero sum game model along with the IoT specific contextual factors, as shown in Figure 5.5. This is because the non-zero sum game theory has modeled the number of interactions between players; by the DODAG structure, it distinctively differentiates the dropping due to network collision from the malicious nodes and identifies the malicious nodes with greater accuracy. The detection accuracy of both the works degrade with the increase in the number of nodes, as shown in Figure 5.5 since the combined strategies of parent selection with a reduced number of interactions degrade the detection accuracy slightly. For example, the S-MODEST achieves 87% of detection accuracy with five malicious nodes over 30 node topology, but it decreases to 80.2% when the network scenario has 60 numbers of nodes. Moreover, when the malicious nodes increase, the detection accuracy of both the S-MODEST and SecTrust gets declined.

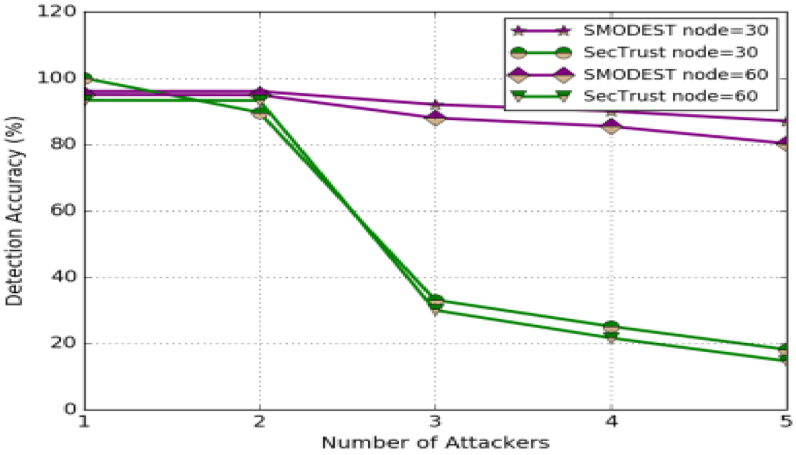

Figure 5.5: Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Detection Accuracy

The proposed S-MODEST is more confident about the trust value as it takes into account the context information and the optimal number of evidence, compared to the SecTrust. As shown in Figure 5.6, the throughput degradation is also reasonable, due to the selection of secure routing path which may have more number of hops to reach the gateway node.

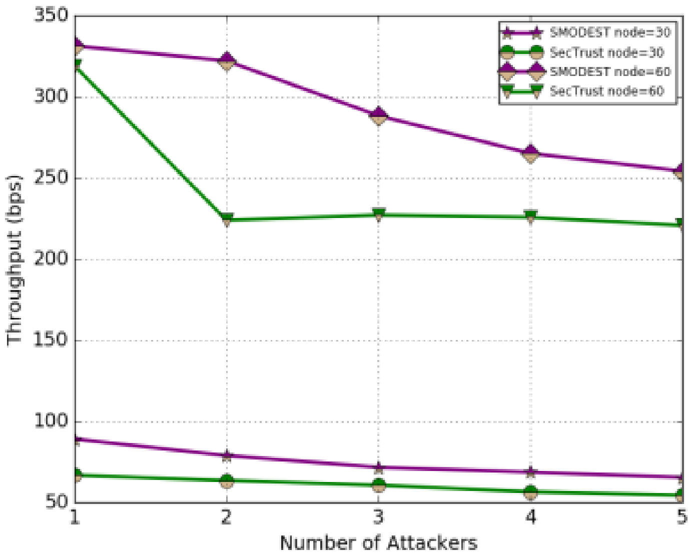

Figure 5.6: Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Throughput

The effects on the normalized overhead are shown in figure 5.7. The normalized overhead is about 3.8 and 5.03, while the nodes and malicious nodes are about 60 and 5, respectively. The dense environment reflects the high rate of requests for indirect trust estimation, resulting in the high overhead. If the performance of S-MODEST is compared with the SecTrust, when the malicious nodes are from 1 to 5, the normalized overhead gets increased. The reason is that the drop in a huge number of data packets tends the normalized overhead to build up. Even though the number of delivered packets increases with the 60 node topology, Figure 5.7 does not show much difference, since the overhead value is normalized. However, the SecTrust collects trust evidence from all the nodes periodically. Accordingly, the SecTrust tends to increase the energy consumption with every addition in the malicious nodes, as shown in Figure 5.8.

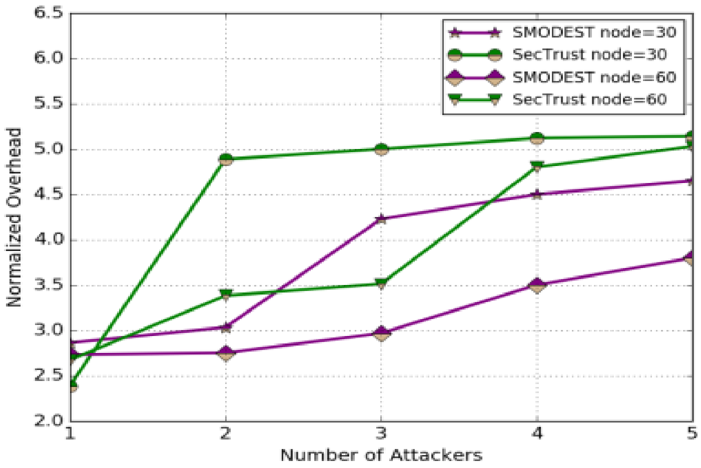

Figure 5.7: Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Normalized Overhead

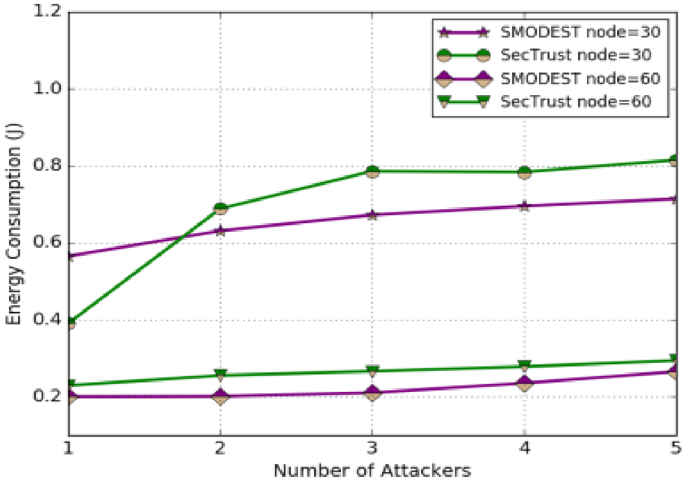

Figure 5.8: Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Energy Consumption

Figure 5.9 demonstrates the route enforcement of S-MODEST using the evolutionary game model. The route enforcement of S-MODEST degrades with the number of attackers and attackers dropping ratio. When the dropping behavior of a node is low, it has less possibility of being a malicious node. The route enforcement using the evolutionary game theory model is high for the S-MODEST with less dropping behavior and 30 node topology. For instance, the S-

MODEST with 0.8 dropping behavior attains 31.4% over 30 node topology, whereas in the same scenario with 60 node topology, it reaches 21.45% of route enforcement.

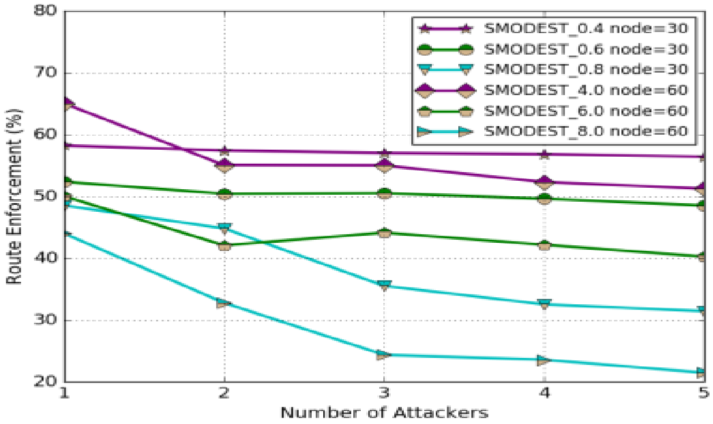

Figure 5.9: Performance Evaluation of S-MODEST by Varying the Number of Attackers in terms of Routing Enforcement

Performance Analysis by Varying Data Interval: Figure 5.10, Figure 5.11, Figure 5.12, and Figure 5.13 shows the performance results of basic S-MODEST and SecTrust by varying the data interval from 10 to 30 seconds. From figure 5.10 and Figure5.11, it is observed that high traffic with low data interval has a profound impact on the protocols. The small data interval enables the non-zero sum game theory to formulate a number of interactions and improves the accuracy of malicious detection. The detection accuracy and throughput of S-MODEST are always better than those of SecTrust, due to the consideration of DODAG and RPL specific features. With the help of more number of interactions, both the S-MODEST and SecTrust attempt to reduce the attacker's impact as well as to measure the accurate trust value. Increasing the data interval escalates the chance of false-positive rate in SecTrust, which does not adapt the detection scheme to the IoT scenario, resulting in more reduced detection accuracy. For example, the detection accuracy of S-MODEST is reduced by 9% when increasing the data interval from 10 to 15 seconds.

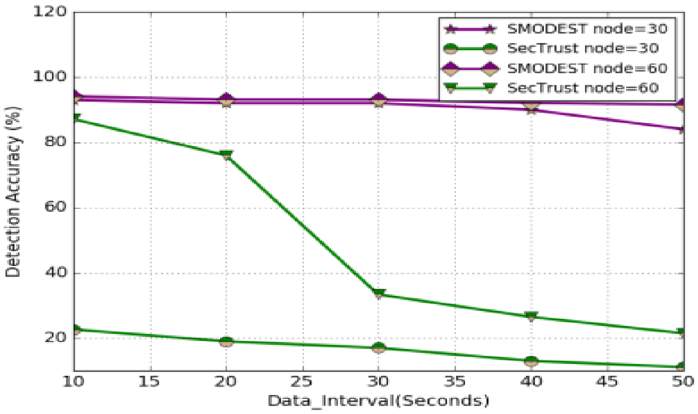

Figure 5.10: Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Detection Accuracy

The throughput of S-MODEST is high compared to existing SecTrust. This is because the SecTrust enables the node to collect evidence from all the neighboring nodes. In the case of falsified trust evidence, the estimated trust is unreliable, and all the transmitted packets through malicious path are dropped. From figure 5.11, the throughput decreases from 670.23 bps to 189.6 bps with 30 node topology, due to the restricted input traffic. Due to the same reason, the energy consumption of Sec-Trust degrades with the data transmission interval, as shown in figure 5.13. The simulation results of overhead in S-MODEST are explained in Figure 5.12. From the figure, it is observed that the S-MODEST achieves the best performance, as it does not require many requests and response packets to measure the indirect trust value. Moreover, the usage of the highly trusted path reduces the frequency of DODAG construction, resulting in less overhead. However, increasing the data transmission interval restricts the number of interactions and escalates the necessity of trust exchanges. As the normalized overhead is being the ratio of control packets over data packets, the reduction in data packets impacts the normalized overhead. For instance, the normalized overhead of S-MODEST with the data interval of 50 seconds is nearly 4.5 on 30 node topology, but with 60 nodes topology, the S-MODEST hikes the overhead to 5. Although S-MODEST requires several control packets with extended data interval, it reduces energy consumption. Since the data packets transmitted to the gateway per second are decreased, the energy consumption of S-MODEST tends to degrade. This is due to the energy consumption of a node to transmit the data packets is a little higher than the control packets.

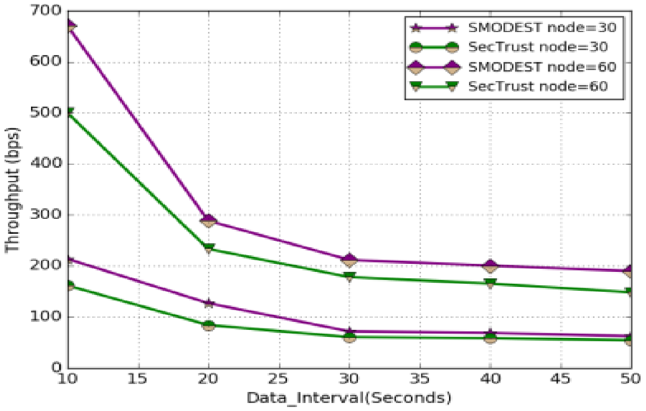

Figure 5.11: Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Throughput

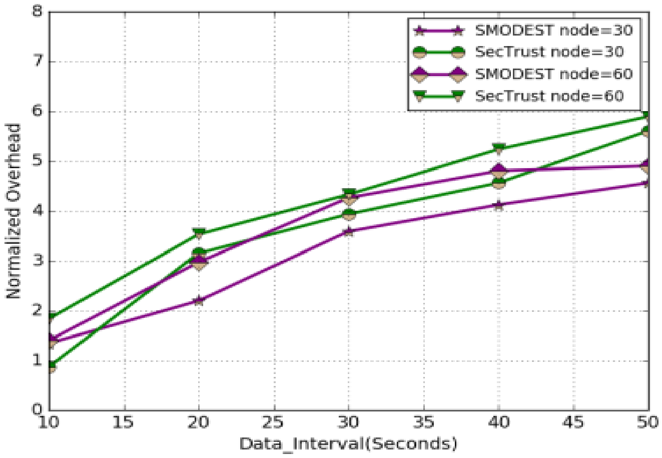

Figure 5.12: Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Normalized Overhead

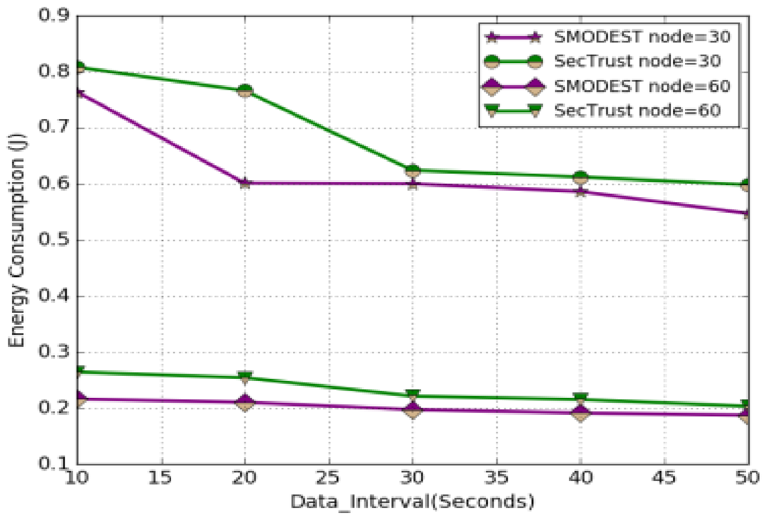

Figure 5.13: Performance Evaluation of S-MODEST by Varying the Data Interval in terms of Energy Consumption

However, with a large number of nodes, Figure 5.13 depicts less energy consumption of S-MODEST in performance due to the transmitted data packet through the same parent node increases drastically on 30 node topology.

SUMMARY

Chapter 5 presented the proposed game theory-based attack detection mechanism called S-MODEST model on the RPL network. Initially, the impact of the malicious dropping attack in the RPL network and the role of the game theory model in RPL security are discussed. The game model formulation of the S - MODEST mechanism is explained. Then, the hostile environment and the utility function are determined. Then, the overview of the S - MODEST model is explained in detail. The direct trust measurement and Dempster-Shaffer Theory-based limited evidence collection are derived. The utility of different strategies and nash equilibrium are explained. Then, the malicious attack detection by using RPL-specific contextual trust measurement is discussed. The trusted DODAG formation using the evolutionary game model is also explained. Finally, the performance comparison between the proposed S-MODEST model and the existing SecTrust model is presented.