The Scientific Temper (2025) Vol. 16 (5): 4181-4189
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2025.16.5.03
https://scientifictemper.com/

RESEARCH ARTICLE

Trust-based symmetric game theory for physical layer security in wi-fi communication

S. Mohamed Iliyas[1], M. Mohamed Surputheen[2], A.R. Mohamed Shanavas[3]

Abstract

A major improvement in the growth of cellular networks has been observed in recent years, being an integral part of the Internet as well as showing reliability in connectivity for decreased military applications and public LANs. This is primarily because of their versatility as well as fewer cost solutions; however, they are also vulnerable to a range of attacks relating to data privacy, denial of service, as well as eavesdropping. To withstand the security demand for wireless communication, this paper presented a trust-based game theory (TRUST-GT). The proposed TRUST-GT introduces confidence assessment for the development of protected routing topology. Consider PDR, energy consumption and throughput; comprehensive simulations demonstrate that it is efficient. We formally characterize TRUST-GT as a method for iterated as well as demonstrated its co-operation compliance characteristic by using game theory principles. The findings of both mathematical analyses as well as evolutionary simulations demonstrate that TRUST-GT is an important tool for fostering the reliability and evolution of Wi-Fi security.

Keywords: Wi-Fi, Direct trust, Indirect trust, Symmetric game theory, Authentication, Routing.

Introduction

Wireless networks have been an important networking platform in recent years, owing to their versatility, reliability and low costs (Alazrai *et al.*, 2020). On the other hand, cellular networks have certain limitations on conventional networks, like limited storage data and low power usage. Moreover, using radio waves, wireless networks transmit data that are vulnerable to eavesdropping. To find unauthorized parts from material, it is significant to keep data transmission through network nodes, which are permanently encrypted. Protocols used to encrypt communications are WPA2 (Wi-Fi Protected Access 2), WPA (Wi-Fi Protected Access) and WEP(Wired Equivalent Privacy) which is governed by cellular network communication management.

Given their shortcomings, however, security technologies designed for such networks are becoming inadequate to deter attacks on secret keys. The purpose of this analysis is to identify security concerns associated with wireless networks. Apart from this, Wi-Fi network consists of anonymous users, which are highly challenging for Wi-Fi security.

Proper operation of the network requires trusting the objects involved in the routing process. In the establishment of trust relationships between participating nodes for stable network operations (Arora & Khera, 2015), cooperation and coordination are considered essential. Cooperation improves optimism and confidence is about the ability to anticipate another party's actions, so cooperation makes predictions more accurate. Symmetric connectivity was regarded in this scenario as an effective strategy for achieving collaboration diversity advantage over wireless communication networks to improve device coverage and link reliability (Chen *et al.*, 2018). Cooperation facilitates the

[1]Research Scholar, Department of Computer Science, Jamal Mohamed College (Autonomous), [Affiliated to Bharathidasan University], Tiruchirappalli – 620 020, India.

[2]Associate Professor, Department of Computer Science, Jamal Mohamed College (Autonomous), [Affiliated to Bharathidasan University], Tiruchirappalli – 620 020, India.

[3]Associate Professor, Department of Computer Science, Jamal Mohamed College (Autonomous), [Affiliated to Bharathidasan University], Tiruchirappalli – 620 020, India.

***Corresponding Author:** S. Mohamed Iliyas, Research Scholar (Part Time), PG and Research Department of Computer Science, Jamal Mohamed College (Autonomous) (Affiliated to Bharathidasan University), Tiruchirappalli, Tamilnadu, India, E-Mail: iliyasjmc@gmail.com

How to cite this article: Iliyas, S.M., Surputheen, M.M., Shanavas, A.R.M. (2025). Trust-based symmetric game theory for physical layer security in wi-fi communication. The Scientific Temper, **16**(5):4181-4189.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.5.03

Source of support: Nil

Conflict of interest: None.

Received: 09/03/2025 **Accepted:** 14/04/2025 **Published** : 31/05/2025

exchange of data by multiple remote devices, generates a shared world, and thereby provides an increased risk or reduced likelihood of loss. Simple actions, such as whether and how to collaborate, can be made by a logical user. However, this Symmetric scenario is subjected to several security constraints for an increased number of attacks. For radio resource management, evaluating the actions of reasonable users and allocating resources and bandwidth pose challenges to meet consumer needs and maximize device efficiency. The theory of games has been suggested as a potential method to model interactions between autonomous users. As a sort of symmetric game model, the bargaining principle has been widely debated for its utility and justice performance (Djedjig *et al.*, 2020). This research developed a trust-based game theory method for security improvement in Wi-Fi networks. Game theory provides arithmetic and concepts for examining strategic decision-making for multiple individuals in which players or DMs compete with limited and shared resources. Security games examine the interplay of malevolent aggressors with defenders in a specific scenario. Security games and their answers are used to decide and build algorithms and forecast attacker behaviour formally. The security game can vary from simple deterministic to complicated stochastic and limited formulations and can be used to address a range of security challenges from intrusion detection to confidentiality and encryption on Wireless, vehicles, and computer networks depending on the type of information available to the DMs, the space of action, and the goals of DMs.

TRUST-GT allows secure routing, by ignoring malicious nodes and selecting most trustworthy router from source node to route. To enhance the identification of untrusted nodes, TRUST-GT allows nodes to collaborate, and thus to implement routing protection. Therefore, TRUST-GT can be seen as a tactic under which the penalty system (i.e. untrusted node isolation) is implemented to empower Symmetric nodes. The performance of proposed TRUST - GT is comparatively examined with existing technique.

This paper is organized as follows: In section 1 presented about general introduction. In section 2 review related to existent WiFi security challenges and related works. In section 3 presents research methodology for proposed TRUST-GT mathematical derivation along with trusty node selection. In section 4, performance analysis with some comparison based on statistical analysis of traffic amount with result discussion and conclusion.

Related Works

Deniable security has been formalized based on cryptography. The imperfection of their verification relies on underlying CCA2 security encryption. Instead of encryption, deniable authentication is constructed with various primitives(Djedjig *et al.*, 2018) .Indeed to create simulation-based deniable authentication, projective hash functions (Khan M. A. *et al.*, 2020) and multi-trapdoor commitment(Huang *et al.*, 2019) are utilized. Also, public random oracle (pRO) (Khan Z. A. *et al.*, 2017) was used to create a deniable protocol for the key exchange (Lahbib *et al.*, 2017). The witness is extracted by pRO in authentication and thereby attains deniability. Based on awareness of the assumption of the exponent (Liu *et al.*, 2011).In which transcripts are perfectly simulated by eliminating witness under KEA presumption, negative Internet key exchange protocols (Louw & Von Solms, 2019) were developed. Tian et al. returned to a modern primitive, selectively unforgettable and existentially forgeable signature (Medjek *et al.*, 2018) for sake of simulation-based rejection.While these methods do not follow a cryptography model (avoiding not efficient CCA2 stable encryption), their underlying primitives communicate on huge assumptions.

The above validation protocols offer complete deniability, meaning that a simulator is run by someone who knows the simulation-based deniability. Partially deniable authentications are also constructed by non-interactive steps when compared with total deniability. Although overhead of contact is the gain, someone should not run the simulator in partial deniability because it clashes with the unforgeability. For instance, in partially deniable authentication, (Mekhaznia & Zidani, 2015), (Nakhila *et al.*, 2018) authentication tag is determined by sender's secret and recipient's public key.The authentication transcript also is estimated by no one but recipient. It allows the authentication to be connected to either the sender or the recipient. If public accepts receiver, it is unacceptable to sender.

Complete deniability demonstrates good secrecy. As communication transcript is simulated by another, recipient cannot persuade 3rd party of sender's presence in verification. During authentication, though the recipient knows the sender. We insist on greater protection of privacy in addition to absolute deniability. The sender is also anonymous to the recipient in privacy-enhanced deniable authentication. By borrowing notion of ring signature that real sender is concealed in a group of representatives, Naor suggested principle of deniable ring authentication (Rizzi *et al.*, 2020). User should then only be persuaded that 1 member of party verifies a message without disclosing which 1. By using CCA2 secure verifiable broadcast encryption, round is lowered to 4 with a commitment to deniable ring authentication (Schulz *et al.*, 2018).

Although Zeng et al. built a deniable ring authentication with 2 rounds (Tang *et al.*, 2019), at cost of PA-secure multi-receiver encryption as well as KEA assumption, their method is successful.It should be remembered that definition of deniable ring authentication varies from that of deniable ring signature (Uras *et al.*, 2020), although they tend to be

identical. The deniable ring signature says that an interactive protocol can be run by a member of a ring (group) who does not sign a message to show that he did not create this signature to refute his participation. On the other side, via a confirmation protocol, the real signer will validate his signature. Nevertheless, it notes that both senders as well as recipient will deny their inclusion in privacy authentication and sender is also invisible to recipient by hiding his name in a group of participants. Deniability is also entirely distinct from this informer.

Construction of TRUST-GT for Wi-Fi Security

To calculate nodes trustworthiness TRUST-GT uses combination of 4 parameters such as honesty, selfishness, energy and ETX.By removing or adding behavioral components, it is flexible and adjustable for WiFi applications. QoS trust component is nodes energy. To achieve its functionalities, expectation level of node i that node j has required energy.Energy trust between node i and node j is percentage of j node ER (Remaining Energy) that is determined from node i denoted by ER_{ij} and ER_{ji} respectively.While receiving and sending packets, nodes consume their energy in WiFi. To estimate energy, there exist various methods.

In (Wei *et al.*, 2011), according to energy model, energy consumed by node i sending k bits data to node *j*, defined by E_i^{mt}, is estimated by using Eq. (1). E_{elec} is electronics energy (i.e., transmitter energyand receiver circuitry), E_{amp} transmitting amplifier energy dissipation, and *d* is node distance from*i* to *j*. Energy consumed by node *j* receiving *k* bits data, indicated by E_i^{mr} is estimated based on Eq. (2). Each node connects with neighbors and transmits information with power level based on nodes communication range for RPL in routing protocol.

Therefore, *d* = Communication range.

$$E_i^{mt} = k*\left(E_{elec} + E_{amp}*d^2\right) \quad (1)$$

$$E_i^{mr} = k*E_{elec} \quad (2)$$

$ER_i(t) = E_{\max}$ i.e., at t=0, $ER_i(0) = E_{\max}$. Sum of energy consumed during transmission is energy spent by node i energy consumed in message reception.Eq. (3) gives remaining energy of node i.

$$ER_i(t) = ER_i(t-\Delta t) - \left(E_i^{mt}(t) + E_i^{mr}(t)\right) \quad (3)$$

Periodically, every node records its neighbor's residual energy.Energy trust value $T_{ij}^{ER} \in [0,1]$ is equal to ratio $ER_{ij}(t)$ and $E_{\max}$ in Eq. (4), where $ER_{ij}(t) = \min\left(ER_{ij}^{reported}(t)\right)$ reported, $ER_{ij}^{estimated}(t)$ and

$$ER_{ij}^{estimated}(t) = ER_j(t)$$

$$T_{ij}^{ER}(t) = \frac{ER_{ij}(t)}{E_{\max}} \quad (4)$$

In Figure 1 presented overall architecture of proposed TRUST-GT for security improvement in Wi-Fi.

d hopping trust values are calculated. The nodes with acceptable trust levels are considered as trusted nodes and minimal trust value is considered as either selfish node or untrusted nodes.

Construction of TRUST-GT for Wi-Fi Authentication

For analyzing interaction between decision-makers, game theory is a significant mathematical theory. It was divided into 2 branches like symmetric and non-symmetric game theory. To maximize its payoff, every player chooses selfishly best method in non symmetric game theory.To come to agreement as well as seek for larger total payoff, all players act symmetrically in symmetric game theory. Symmetric game theory has following elements (Yao *et al.*, 2018):

- Non-empty set of pure strategy for each player
- A finite set of decision-makers, that is, players of game.
- For each player with players strategies, set of payoff functions

Taking into account this symmetrical action, as a symmetrical problem, battle against heterogeneous access networks can be conceived to accomplish networks load balancing and QoS specifications of different applications, and symmetrical game balances are assumed to be a games solution.

Players

In dense urban areas, multiple WiMAX BSs and Wi-Fi APs also have a mobile node concurrently within overlapping coverage areas.Competition between heterogeneous access

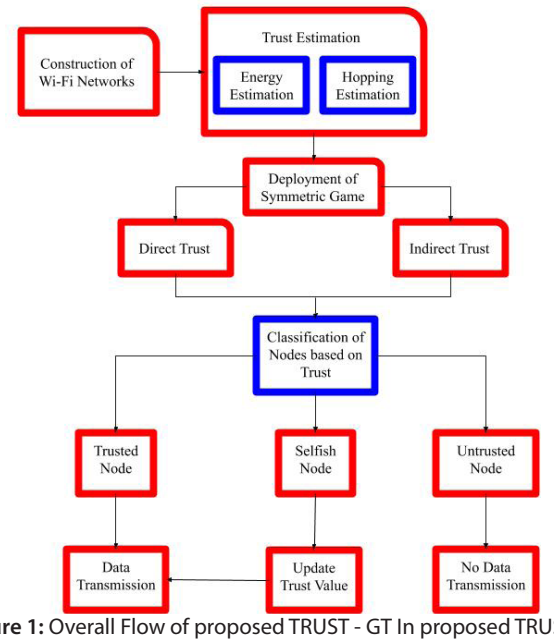

Figure 1: Overall Flow of proposed TRUST - GT In proposed TRUST - GT based on energy an

networks occurs.Game players are described as a finite set $\{B_{S-1}, y, B_{S-n}, A_{P-1}, y, A_{P-n}\}$, where B_{S-n}indicates Wi - Fi, A_{P-n}indicates Wi-Fi AP, etc.Game players are often referred to in biding model as a set of bidders, which is also implemented in previous section.

Finite set s_i¼{b_1, b_2, y, b_n} is strategy of each network in round in which each element is defined as bid concerning bidding model tender. Set S_i¼{si} is all potential plan of every network in which si is defined as networks special strategy in a round. In round all players strategy is denoted as set $\{s_1, s_2, y, s_n\}$, and all players strategies are denoted as set $\{S_1, S_2, y, S_n\}$.

According to (5), every network access payoff function is found by bid. Payoff function of network *i* is denoted asu_i. Value of ui is equal to sum of bids received by APs which chooses network *i*. Total payoff of all access networks is defined as

$$T = \sum_{i=1}^{n} u_i \qquad (5)$$

where *T*indicatesall access networks total payoff, *n*indicates number of game players. Thus, Symmetric game methodis$G$¼$\{n; S_1, y, S_n; u_1, y, u_n\}$, where *n*indicates number of game players, and game played in rounds. Each player individually selects his strategy from set Si in each round of the game loop and receives his payoff ui(s1, s2, y, sn). In addition, every player also estimates its network utility, which is described as equation (6):

$$R_i = \frac{UP\_B_i}{T\_B_i} \qquad (6)$$

where $R_i$indicates network utility, UP_B_iindicatesnetwork bandwidth and $T_B_i$denotes networks total bandwidth. Since bandwidth is most valuable and scarce wireless network capital, we also use network utility to indicate traffic load of each connection point for simplicity.

Each network behaves symmetrically as a game player in every round of game loop to seek greater overall payoff, and attempts to attain successful load balancing, that relies on relationship between network utility of every player.In a round game, if one is higher than default value x, balance is not attained, and then next round game begins to be played, as both players symmetrically change their game plan in direction of agreement.Information of how techniques can be tailored in direction of agreement are defined in following manner. To minimize probability of winning a bid, a higher network usegamer will raise the bid. To maximize probability of winning a bid, a player with a lower network use will reduce bid. It completes load balance after restricted rounds and obtains a greater overall payout.

Estimation of Trust value in Nodes

While attempting to consume other resources, selfish node intends to limit their expenditure. Nodes selfishness is calculated as collaborative and distributed score. During period P, node i calculates node j and determines if node j is selfish or not by utilizing methods like snooping and overhearing (Zeng *et al.*, 2020). Let us consider application needs less energy indicated by $E_{\min}$. If $ER_i(t)$ is higher than $E_{\min}$, node *i* acts correctly; if $ER_i(t)$ is less or equal to $E_{\min}$, it does not take part in forwarding packets any longer and uses, for instance, its energy for transmissions of its packets, which implies it is more likely to become selfish. To save their resources, TRUST – GT allows some degree of nodes selfishness during trust calculation stage. Nodes determine trade-off between selfishness and energy based on this method.

To estimate selfishness, this paper has 2 types of packets:

Control packets

And where nodes have low energy levels and self-trust is 0, when node drop control packets are assumed to be malicious.To preserve routing topology, drop control packets are not tolerated because they are important.

Data packets

Data packets are estimated based on two parameters such as normal energy level and low energy level.

Normal energy levels

Forprogram execution $ER_{ij}(t) > E_{\min}$, if nodes lose data packets in which remaining energy is higher than minimum needed energy, selfishness count -N- is increased (i.e., N=N+1).If N exceeds criterion of selfishness, then node is called selfish.

Low energy levels

due to fewer energy levels, node drops data packets, count number of selfishness -Nis not increased, which means node is not taken as selfish.

Using Eq.(7), nodes selfishness is calculated in which N indicates reset at end of period P.

$$T_{ij}^{selfish,new}(t) = \begin{cases} 0 & ifN(t) \geq T_{selfish} \\ 1 - \frac{N(t)}{T_{selfish}} & else \end{cases} \qquad (7)$$

Selected Trusty Nodes by TRUST-GT

Determine whether node is malicious or not, honesty parameter signals are used. To find if node j is adjusted or not, node I calculate node j behavior. Depends onset of anomaly detection rules, some methods use IDS (Intrusion Detection System) [21]. To detect and monitor malicious behaviors, each node i executes an IDS in TRUST-GT.As IDS activates a node j alert, node i monitoring finds node j deceptive as well as assigns an honesty-trust-value of 0 to it as in Eq. (8).

Information on IDS identification attacks is beyond reach of this article.

$$T_{ij}^{Honesty,new}(t)=\begin{cases}0 & \text{if node j malfuction}\\ 1 & \text{else}\end{cases} \quad (8)$$

Trust Evaluation of Wi-Fi nodes with TRUST - GT

Trust value of nodes in TRUST-GT method is a mixture of both indirect recommendations and direct observation.

Direct trust

At time t each node estimates trust value $T_{ij}(t)$ of its 1-hop neighbor.Trust value of an entity like Bayesian systems, weighted sum,Fuzzy logic and belief theory are calculated using several methods.To evaluate nodes' trustworthiness, weighted sum method is chosen due to RPL's objects have processing capacity and less storage.Eq.(9) gives measured direct confidence in which w1, w2, w3 and w4 are weights with honesty, energy, selfishness and ETX. Eq. (10) indicates evaluate every behavioral specification $X \in \{Honesty : Selfish\}$, where Δt is trust update interval, $T_{ij}^{X}(t-\Delta t)$ is old observation $\alpha \in [0,1]$ .Trust depends more on new findings, whether it appears to be 1.Esteem, otherwise, depends more on old findings, if a tends to 0.

Because residual energy represents capacity of node to attain its functionality as well as ETX reflects status of connection, confidence measurement for each is focused solely on new observations.

$$\begin{cases}T_{ij}^{Direct}(t)=w_1T_{ij}^{Honesty}(t)+w_2T_{ij}^{Selfish}+w_3T_{ij}^{ER}(t)+w_4T_{ij}^{ETX}(t)\\ w_1+w_2+w_3+w_4=1\end{cases} \quad (9)$$

$$T_{ij}^{X}(t)=\alpha T_{ij}^{X,new}(t)+(1-\alpha)T_{ij}^{X}(t-\Delta t) \quad (10)$$

Indirect Trust

Since TRUST - GT is a symmetric mechanism aimed at choosing most secure path to root, the node i uses trust values obtained from its neighbors k.After evaluating direct trust, final trust value of node j is determined for each node j, as in Eq (11).As indicated by Eq. (9), last trust esteem is normal of direct trust esteem assessed and all suggestions got for that node j in ERNT objects.

$$T_{ij}(t)=\frac{T_{ij}^{Direct}(t)+\sum_k T_{kj}^{\mathrm{Re}com}(t)}{|k|+1} \quad (11)$$

If node i receives suggestions for nodes which are not 1-hop neighbors, they will be overlooked.Either periodically or reactively, TRUST - GT updates trust values.Periodic trust updates are time-driven, using a trickle timer to relay messages from DAG (DIO) data object as a regulator, while reactive trust updates are event-driven, using triggers for global and local repair events.Global or local pair is triggered when IDS produces an alarm (i.e., it finds an attack) or if $T_{selfish}$ is reached. Or else, trickle timer monitors update.

At the point when a node i gets DIO messages from its neighbors, it changes its routing table by utilizing information from DIO messages.Using direct recommendations and assessments received in DIO messages, it estimates neighbors' trust values. To reach BR, it chooses selects set of trusted parents.It determines path cost through every possible parent as well as selects one with high-cost value of path as a chosen parent, ensuring most trustworthy as well as efficient traffic routing to BR. For each of its neighbors, it generates as well as broadcasts new DIO message which contains calculated trust values. Until DODAG (Destination Oriented Directed Acyclic Graph) is reconstructed, all neighboring nodes repeat process. Maintenance starts after trickle timer, once construction is completed. Transmission rate of control messages is regulated by timer.In stable state, trust trickle time interval increases and less transfer rate which shows less computation and control messages which has less energy consumption, CPU and memory.Otherwise, where there are contradictions around topology changes (e.g. attack discovery, greedy operation identification, and a new node entering DODAG), Trickle timer would be reset to less value then rate of transmission is unchanged, meaning huge control messagesas well as computation.TRUST - GT smoothes out a minor path expense low or rise to reduce estimation cost regarding energy usage generated by confidence upgrade overheads.To avoid frequent parent changes to conserve energy and maintain stability, consider hysteresis threshold of 0.15.

Proposed TRUST-GT algorithm was presented below:

Algorithm 1: Constructed TRUST - GT method

Require: *NodesList, NeighboursList,* T_{Trust}, $T_{Selfish}$, w_1, w_2, w_3, w_4, α, P
Ensure: *PreferredParent, Rank*
if *NeighboursList= ∅* ***then***
Construct topology according to TRUST - GT
else
while *1* ***do***
if *ERNT.T=0 (passive mode)* ***then***
Construct topology according to TRUST - GT
else *{ERNT.T=1 (active mode)}*
for all *j ∈ NeighbourList* ***do***
(Calculate Direct Trust)
Activate Promiscuous mode, watchdog mechanism, and IDS
Compute trust value of node for routing data
Update Trust Table
end for
for all *j ∈ NeighbourList* ***do***
(Calculate Indirect Trust using recommendations)
Update Trust Table: ($T_{ij}(t)$)
Update ParentList ($T_{ij}(t) \geq T_{Trust}$)
end for
From ParentList, Select $T_j(t)$ with greater PC_i
Update Rank if ($PC_i - PC_{Actual\text{-}Parent} > 0.15$)
Build DIO with calculated values and forward
end if
end while
end if
return

Table 1: Simulation Parameter

Parameters	*Values*
Simulator	NS 2
Simulation Time	80ms
Traffic rate	1 packet sent every 10 seconds
Range of nodes	RX: 50%, TX: 50m, interference: 60m
T_{Trust}	0.5
A	0.75
w1, w2, w3 and w4	0.25

Results and Discussion

Lightweight and open source NS2 simulator is used for simulations [39]. Performance is evaluated for changing number of nodes in center of BR and around BR 29 skymote (TelosB) is placed randomly. Trust threshold is set as T_{Trust} to 0.5 and α to 0.75 for simulation. First, we set weightsw_1, w_2, w_3 and w_4 equally to 0.25, due to all 4 factors are equally significant to choose secure routes which have good QoS.As this analysis focuses on security concerns for RPL routing, during evaluation, when IDS identifies a node as malicious, regular nodes change weights associated with MN by setting w1 to 1 and w2, w3 and w4 equal to 0. Normal nodes can adjust weights of selfish nodes by setting w2 to 1and w_1, w_3 and w_4 equal to 0, when node finds another node as selfish. Table 1 indicates simulation parameters.

The performance of proposed TRUST - GT is comparatively examined with existing techniques such as LWR and SWISH. The performance metrics considered for analysis are energy consumption, accuracy, throughput and packet loss ratio. The simulation measurement is conducted for 80ms with varying number of users.

Energy Consumption

The use of energy within the sensor node depends on the average node power consumption in the operation time.

$$\text{Energy Consumption (EC)} = \frac{\sum(Numberofpacketssent)\times(SE+PE)}{1+(Numberofpacketsreceivedbysink)\times(\Re+PE)}$$

WhereSE is Sending Energy. PE is Processing Energy, RE is Residual Energy.

Some nodes use more resources than others in TRUST - GT network because they tend to be picked more often as a chosen parent based on their ETX; this is a concern because higher energy costs of selected parents influence lifespan of entire network.Table 2 shows comparison of energy consumption in TRUST-GT in which nodes consume more energy due to rank changes as well as topology instability under attacks.

In Figure 2, presents about energy consumed for proposed TRUST - GT comparatively with existing technique. Between various nodes, TRUST-GT has better energy consumption is much more balanced.

Table 2: Comparison of energy consumption

Nodes	*LWR*	*SWISH*	*TRUST-GT*
0	0	0	0
20	18.78	14.87	9.57
40	29.57	21.85	15.67
60	35.86	28.53	21.63
80	45.67	37.83	29.50
100	46.87	38.66	30.76

TRUST-GT performance in terms of energy consumption because of fact that it considers each node remaining energy in routing decisions.Energy consumption rate decreases and topology becomes more stable when malicious nodes are detected and isolated, TRUST-GT consumes most energy in DIO transmissions and calculation. Node selects one which is having highest remaining energy when two candidate parents have same trust value which is already stated. When comparing with existing methods the proposed TRUST-GT achieves 30.76% for 100 number of nodes

In Table 3, comparative analysis of proposed TRUST - GT with existing technique LWR and SWISH and SWISH are presented.

In Figure 3, the energy efficiency of the proposed TRUST-GT is illustrated for varying numbers of nodes.

From Figure 3, it is observed that energy efficiency of proposed TRUST - GT is effective for number of times. The energy consumption of proposed TRUSTv - GT is minimal which in turn increases the energy efficiency rather than LWR and SWISH and SWISH. When comparing with existing methods the proposed TRUST-GT achieves 81.59% of energy efficiency for 100 number of nodes

Table 3: Comparison of Energy Efficiency

Nodes	*LWR*	*SWISH*	*TRUST-GT*
0	100	100	100
20	88.67	91.67	96.53
40	77.87	81.78	91.87
60	62.68	72.86	86.68
80	55.83	63.57	81.59

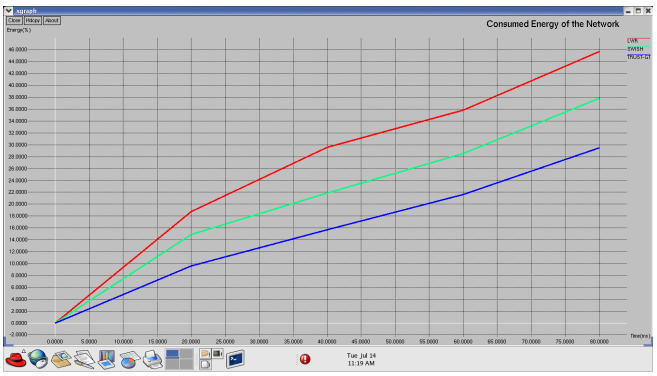

Figure 2: Comparison of Energy Consumed

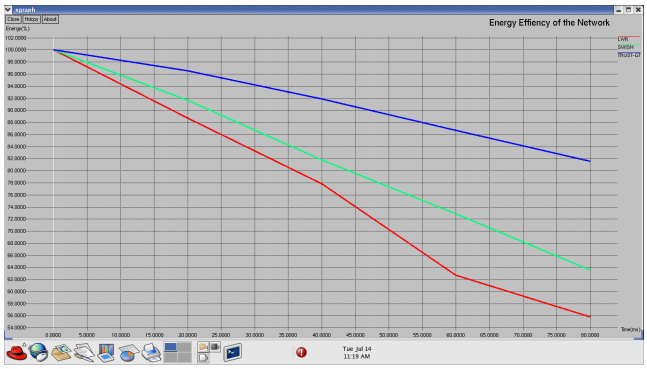

Figure 3: Comparison of Energy Efficiency

Packet Delivery Ratio

Packet delivery ratio is the average ratio of the totalpackets accepted successfully to the total packets originally sent.

$$\text{Packet delivery ratio} = \frac{\sum numberofpacketreceive}{\sum numberofpacketsend}$$

Figure 4 shows network congestion and packet collision.

It is observed from Figure 4 that when normal node selects malicious node to forward its packets as a preferred parent, latter which delete control packets that make topology unstable as well asunavailable.TRUST-GT, on other hand kept PDR very high (up to 90 percent) because it utilizes IDS to determine attacks as well asgives a new routing method to separate MN (Malicious Nodes)as well askeepingsecure topology. Attacks on TRUST-GT cause major damages. Compared to SWISH and LWR it shows better PDR. It minimizes rank changes rate and gives more stable network in SWISH and LWR and also minimizes packet loss.When comparing with existing methods the proposed TRUST-GT achieves 89.59% of PDR for 100 number of nodes

In Table 4, accuracy measurement for varying numbers of nodes is presented along with comparison with existing techniques such as LWR and SWISH and SWISH.

In Figure 5, comparative analysis of measured accuracy value of proposed TRUST - GT with existing technique is presented.

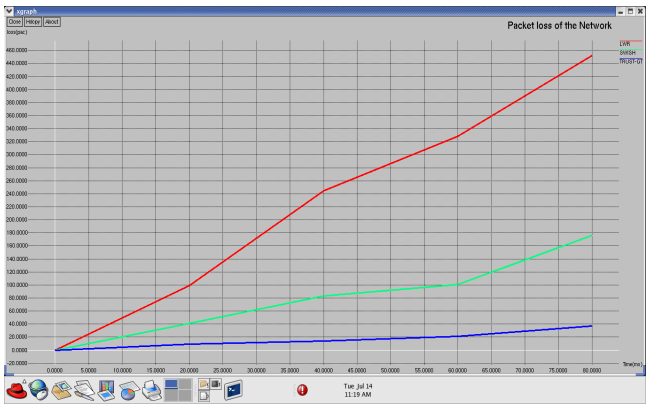

Figure 4: Comparison of Packet Loss

Table 4: Comparison of Accuracy

Nodes	*LWR*	*SWISH*	*TRUST-GT*
0	0	0	0
20	12.53	16.89	21.87
40	18.67	25.62	29.57
60	46.57	49.57	53.67
80	59.46	71.57	79.52
100	72.67	83.78	97.23

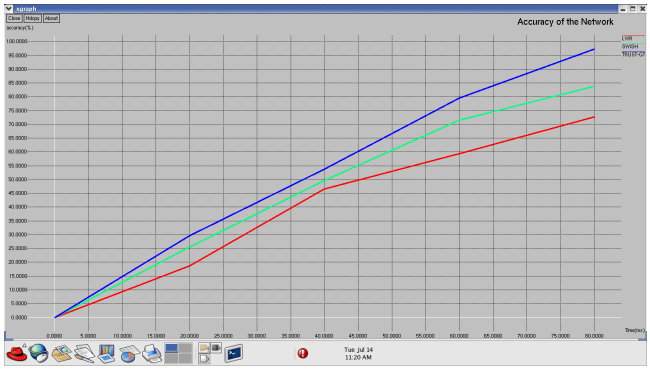

Figure 5: Comparison of Accuracy

From Figure 5, it is observed that proposed TRUST - GT offers higher accuracy rather than existing technique.When comparing with existing methods the proposed TRUST-GT achieves 97.23% of accuracy for 100 number of nodes

Throughput of Network

Throughput is the rate of data flow through a channel used for communication i.e. bits or packets delivered successfully over a channel in the network.

$$\text{Throughput (bits/sec)} = \sum \frac{(\text{numberofsuccessfulpackets}) * (\text{averagepacketsize})}{\text{TotalTimesentindeliveringthatamountofdata}}$$

In table 5 comparative measurement of throughput is provided along with varying numbers of nodes.

In Figure 6, comparative analysis of proposed TRUST - GT with existing techniques is presented.

Figure 6 shows TRUST-GT throughput in case of rank attacks and black holes which is highly reduced when compared to SWISH and LWR. In SWISH and LWR, threats

Table 5: Comparison of Throughput

Nodes	*LWR*	*SWISH*	*TRUST-GT*
0	0	0	0
20	28.57	57.26	76.67
40	51.25	103.28	129.57
60	78.56	139.78	187.57
80	88.68	153.57	224.29
100	103.68	163.57	264.29

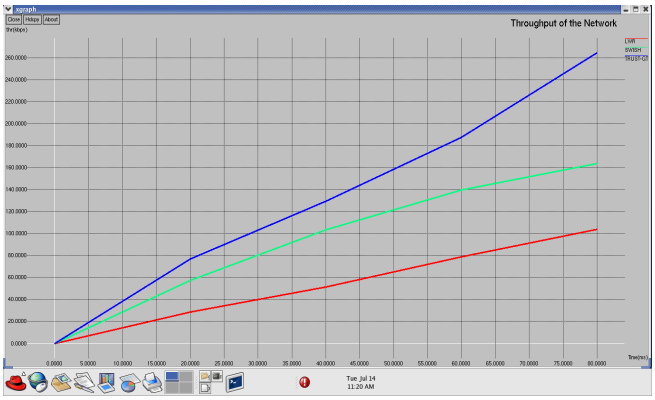

Figure 6: Comparison of Throughput

are detected and malicious nodes are isolated. Overall throughput increases when all node's throughput is greater than zero.When compared with SWISH and LWR, throughput of TRUST-GT is better as similar to PDR and it provides more stable network when compared to others and reduces packet loss and increases throughput.When comparing with existing methods the proposed TRUST-GT achieves 264.29 kbps of throughput for 100 number of nodes.

Conclusion

For RPL, a cooperation trust-based routing method called TRUST-GT was proposed in this paper.According to TRUST - GT, as its preferred parent at every hop of RPL routing, child node chooses nodes with huge trust value, energy and connectivity quality.To minimize network security risks as well as maintain its stability and performance, we demonstrate through simulation that game theory of TRUST-GT is significant routing method. Having capacity to detect as well as isolate attacks and energy balanced topology method as well as it has high PDR and low energy consumption. Moreover, it is translated to strategy using game theory concepts. To cooperate rather than to cheat, it forces network by forcing nodes and punishes as well as isolates unsymmetric (untrusted) nodes. The analysis of the cooperation evolution of TRUST - GT strategy as well as demonstrated. From analysis it is concluded that proposed TRUST - GT provides increased accuracy, throughput and energy efficiency.

Acknowledgements

The authors would like to express their sincere gratitude to Jamal Mohamed College for providing the necessary facilities and support to carry out this research work. We also thank our college management, heads, co-researchers, colleagues and reviewers for their valuable feedback and constructive suggestions, which greatly improved the quality of this manuscript.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

Alazrai, R., Awad, A., Baha'A, A., Hababeh, M., & Daoud, M. I. (2020). A dataset for Wi-Fi-based human-to-human interaction recognition. *Data in Brief*.

Arora, A., & Khera, A. (2015). Wi-Fi enabled personal computer network monitoring system using smartphone with enhanced security measures. *Procedia Computer Science*, *70*, 114–122.

Chen, R., Guo, J., Wang, D. C., Tsai, J. J., Al-Hamadi, H., & You, I. (2018). Trust-based service management for mobile cloud IoT systems. *IEEE Transactions on Network and Service Management*, *16*(1), 246–263.

Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2020). Trust-aware and cooperative routing protocol for IoT security. *Journal of Information Security and Applications*, *52*.

Djedjig, N., Tandjaoui, D., Romdhani, I., & Medjek, F. (2018). Trust management in the Internet of Things. In *Security and Privacy in Smart Sensor Networks* (pp. 122–146).

Huang, W., Lin, Y., Lin, B., & Zhao, L. (2019). Modeling and predicting the occupancy in a China hub airport terminal using Wi-Fi data. *Energy and Buildings*, *203*.

Khan, M. A., Hamila, R., Al-Emadi, N. A., Kiranyaz, S., & Gabbouj, M. (2020). Real-time throughput prediction for cognitive Wi-Fi networks. *Journal of Network and Computer Applications*, *150*.

Khan, Z. A., Ullrich, J., Voyiatzis, A. G., & Herrmann, P. (2017). A trust-based resilient routing mechanism for the Internet of Things. In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (pp. 1–6).

Lahbib, A., Toumi, K., Elleuch, S., Laouiti, A., & Martin, S. (2017). Link reliable and trust aware RPL routing protocol for Internet of Things. In *IEEE 16th International Symposium on Network Computing and Applications (NCA)* (pp. 1–5).

Liu, X., Fang, X., Chen, X., & Peng, X. (2011). A bidding model and cooperative game-based vertical handoff decision algorithm. *Journal of Network and Computer Applications*, *34*(4), 1263–1271.

Louw, C., & Von Solms, B. (2019). Free public Wi-Fi security in a smart city context—An end user perspective. In *Smart Cities Cybersecurity and Privacy* (pp. 113–127).

Medjek, F., Tandjaoui, D., Romdhani, I., & Djedjig, N. (2018). Security threats in the Internet of Things: RPL's attacks and countermeasures. In *Security and Privacy in Smart Sensor Networks* (pp. 147–178).

Mekhaznia, T., & Zidani, A. (2015). Wi-Fi security analysis. *Procedia Computer Science*, *73*, 172–178.

Nakhila, O., Amjad, M. F., Dondyk, E., & Zou, C. (2018). Gateway independent user-side Wi-Fi Evil Twin attack detection using virtual wireless clients. *Computers & Security*, *74*, 41–54.

Rizzi, A., Granato, G., & Baiocchi, A. (2020). Frame-by-frame Wi-Fi attack detection algorithm with scalable and modular machine-learning design. *Applied Soft Computing*.

Schulz, M., Wegemer, D., & Hollick, M. (2018). The Nexmon firmware analysis and modification framework: Empowering researchers to enhance Wi-Fi devices. *Computer Communications*, *129*, 269–285.

Tang, X., Tan, Z., Hu, S., & Geng, H. (2019). Evaluating spatial service and layout efficiency of municipal Wi-Fi facilities for SmartCity planning: A case study of Wuhan city, China. *Socio-Economic Planning Sciences*, *65*, 101–110.

Uras, M., Cossu, R., Ferrara, E., Liotta, A., & Atzori, L. (2020). PmA:

A real-world system for people mobility monitoring and analysis based on Wi-Fi probes. *Journal of Cleaner Production*.

Wei, L. I. U., Tao, L. U. O., & Yue, G. X. (2011). Dynamic subcarrier and power allocation based on cooperative game theory in symmetric cooperative OFDMA networks. *The Journal of China Universities of Posts and Telecommunications*, *18*(2), 9–16.

Yao, M. L., Chuang, M. C., & Hsu, C. C. (2018). The Kano model analysis of features for mobile security applications. *Computers & Security*, *78*, 336–346.

Zeng, S., Mu, Y., Zhang, H., & He, M. (2020). A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy. *Information Sciences*, *516*, 331–345.