Hidden Markov Trust for Attenuation of Selfish and Malicious Nodes in the IoT Network

Gamini Joshi
Gautam Buddha University
Vidushi Sharma (vidushisharma2021@gmail.com)
Gautam Buddha University

Research Article

Keywords: Internet of Things (IoT), Trust Management, Hidden Markov Model (HMM), Selfish node, malicious node, network survivability

Posted Date: September 21st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-776578/v1

Hidden Markov Trust for attenuation of selfish and malicious nodes in the IoT network

Gamini Joshi[1], Vidushi Sharma[2*]

Abstract

The exposure of IoT nodes to the internet makes them vulnerable to malicious attacks and failures. These failures affect the survivability, integrity, and connectivity of the network. Thus the detection and elimination of attacks in a timely manner become an important factor to maintain the network connectivity. Trust-based techniques are used in understanding the behavior of nodes in the network. Several researchers have proposed conventional trust models that are power-hungry and demand large storage space. Succeeding this Hidden Markov Models have also been developed to calculate trust but the survivability of network achieved from them is low. To improve the survivability selfish and malicious nodes present in the network are required to be treated separately. Hence, an improved Hidden Markov Trust (HMT) Model is developed in this paper which accurately detects the selfish and malicious nodes that illegally intercept the network. An algorithm is generalized for learning the behavior of nodes using the HMT model with the expected output. The evaluated node's likelihood functions differentiate the selfish node from the malicious node and provide independent timely treatment to both types of nodes. Further, comparative analysis for attacks such as black-hole, grey-hole, and sink-hole has been done and performance parameters have been extended to survivability-rate, power-consumption, delay, and false-alarm-rate, for different networks sizes and vulnerability. Simulation result provides a 10% higher PDR, 29% lower overhead, and 15% higher detection rate when compared to FUCEM, FTCSPM, and OADM trust models presented in the literature.

Keywords: Internet of Things (IoT), Trust Management, Hidden Markov Model (HMM), Selfish node, malicious node, network survivability

1. Introduction

The use of the Internet of Things (IoT) in transmitting and sharing data, resources, and services through the internet had won popularity, especially in the areas such as tracking/monitoring, health services, military applications, agricultural, vehicular communications, etc. The issue of maintaining data integrity and network resilience in IoT is considered as the key entity for reliable data communication. But the exposure of IoT nodes to the open-ended side of the internet makes them vulnerable to attacks and breaches, which infects their integrity [1]. Moreover, the behavioral transition of nodes towards the act of selfishness affects the connectivity of the network [2]. Further, IoT devices suffer from random failures due to their distinctive features such as limited memory, limited energy, limited computational capabilities, and decentralized infrastructure. Therefore, for the feasibility and stability of the IoT network, a collaborative environment is favored that should be free from a selfish and malicious act. *Selfish nodes* deny forwarding the data packets of their neighboring nodes; to conserve their energy and the *Malicious nodes (or mischievous)* manipulate the data to damage the integrity of the IoT network.

To protect IoT nodes from attacks, while keeping the network connectivity and integrity intact is a difficult task. The conventional cryptographic methods are not acceptable to resource constraint IoT nodes owing to their code size, processing time, and energy consumption. Therefore, alternate trust-based security primitive mechanisms are proposed like Bayesian systems, fuzzy logic, etc. The survey study demonstrates that these trust evaluation methods are dependent on external parameters like the opinion of neighboring nodes and their past behaviors. Inculcation of these factors calls for large memory and communication overhead. In addition, these approaches present the detection of compromised nodes but lack to discriminate the impact of selfish and malicious activity on the IoT network.

[1] Gamini Joshi
Computer Science Department, School of ICT, Gautam Buddha University, Greater Noida, India
joshi.gamini@gmail.com

[2*] Vidushi Sharma (Corresponding author)
Computer Science Department, School of ICT, Gautam Buddha University, Greater Noida, India
vidushisharma2021@gmail.com

Differentiation of selfish and malicious nodes is needed, since, the objective function of the selfish node is to make routing impossible by never participating and always dropping the packets of neighbor nodes while malicious nodes though always take part in network function but try to damage the flow of data. To counter the effect of these nodes, the immediate impression is to destroy these nodes from the network. Treating both nodes in a similar way though improves effective communication among nodes but directly and indirectly impacts the survivability of the resource constraint IoT network. Hence there is a need to provide a technique that can handle selfish and malicious nodes differently and can mitigate the problems due to it so that the survivability of the network can be improved with effective communication.

In this paper, the dynamic behavior of nodes at any given time is characterized by the probability distribution of the possible outcomes like parameter changes, fault frequency, etc. We have used the Hidden Markov-based trust model (HMM) for capturing the zestful behavior of nodes and forecast the likelihood of the node to be in one of the hidden states (or behavior). The model analyzes the 4-state HMM where states are named as the adaptive, greedy, mischievous, and crashed states and the possible outcomes are the analysis of packet transferal information associated with each interaction. In the context of trust-based applications, any routing protocol for low power and lossy network (LLN) is acceptable like RPL, 6LoWPAN, LOADng, etc. For simplicity of the network, our work is focused on IoT applications where communication among devices is generally peer-to-peer and the node intends to set a trusted path to a destination. Thus, the trusted route discovery is needed, which is triggered by the source node that wants to send the message. Considering this type of scenario, the Lightweight On-demand Ad hoc Distance vector routing protocol (LOADng) is found to be the best protocol to design the proposed model. LOADng is an enhanced version of the Adhoc On-Demand Distance Vector (AODV) routing protocol, which aims to reduce the complexity and the number of computational resources that are required for execution [3]. Therefore, our model constitutes LOADng routing protocol with an additional collaborative metric that discovers the most trustworthy neighbor and designs a fault-tolerant routing path.
The proposed mechanism Hidden Markov Trust (HMT) can be directly used in IoT nodes. The mechanism will be able to intact the integrity and the survivability of the network. Our work strengthens the survivability of the network by the node's energy and providing a temporal opportunity to the uncooperative nodes before their isolation. This is done to increase the performance of the network because generally, the traces of uncooperativeness actions persist for a small duration. Uncooperativeness can exist because of the selfish nature of nodes or malicious nature or it can be when residual energy of node is minimal and it is at the edge of the crashed state. The proposed scheme is different from the conventional scheme in terms of the method used to discriminate against selfish and malicious activity. The scheme seeks to build network performance by giving a time-based opportunity to the infected nodes. Conventional design substantially focuses on immediate mitigation of compromised nodes without analyzing their chances of improvement; thus, drops the survivability rate of the network. The paper contributions are listed below:

1. Development of a structured algorithm: A generalized trust evaluation algorithm has been presented in a structured manner for a node to select the trustworthy and reliable path to the destination. We discuss available parameters that affect the path trustworthiness like available energy, packets drooped, packets modified.
2. Mathematical evaluation and analysis: The maximum likelihood of the node's behavior using the Hidden Markov Approach provides a clear mathematical analysis of cooperative node selection that proceeds by combining transition and emission metrics.
3. Simulation Results: Simulation results are provided to evaluate and compare the best suitable trust model for different network sizes (scalability) and different vulnerabilities (in presence of maliciousness). In addition, the model simulates the sinkhole attack along with the black hole and grey hole attack. Thus, covers all the possible attacks.
4. Performance Evaluations: The potential of the model is estimated for the survivability rate, packet delivery rate (PDR), energy consumption, end-to-end delay, routing overhead, detection rate, together with false positive and false negative factors.
5. Critical Analysis: The advantages and challenges of providing Time Based opportunities to the infected nodes have been addressed and the effect of changing network size in presence of malicious attacks is presented.

The paper is structured as follows: Section 2 presents the related work in the area of detection and elimination of nasty nodes. Section 3, describes the system model for attenuating selfish and malicious activity. Section 4, presents the mathematical model along with an evaluation of trusted node and decision making scenario. Analysis of simulation results and their impact on different performance parameters is provided in section 5.Finally the conclusion and future scope is drawn in section 6.

2. Related work

The security in IoT is conventionally carried out using cryptographic methods, where public key and symmetric key techniques are adopted. As for sensor nodes, both key operations are expensive in terms of computations and energy consumption. Considering this, the study of trust evaluation mechanisms for IoT security has gained momentum. Trust models provide the benefits of lesser resource consumption, peer-to-peer structure, and compromised node detection. Thus, trust is considered to be an important factor to ascertain the survivability of the network.

In recent years, researchers have focused their attention on the stochastic Markov model for providing security from attacks in different areas of technology and applications such as communication, defense, monitoring, etc. Zhongqiu et al. [4] presented a quantitive measure of survivability for the clustered network in presence of DoS attacks. In their work, the authors investigated mechanisms of the Markov chain that categorizes nodes into an active state and a dead state. They have incorporated the evaluation of the degree of services to estimate the probability of the node's state. The approach adds failure rate (active to the dead) in connection with energy consumption of node and repair rate (dead to active) as a measure of node density. To be specific, the author has resolved the DoS attack by increasing the density of the node. Though the model increases the survivability rate the perspective of increasing the node's density effect's the node's residual power.

The applicability of the simple Markov chain model is not always feasible because the transition time from one state to another is a random variable while the former applications use time as an exponential distribution. Therefore, the semi-markov process is highlighted to characterize the node state transition. Advancing further, Theerthangiri [5] recommended a Futuristic cooperation evaluation scheme (FUCEM) for establishing an effective routing path. The work adopts a semi-markov process for determining node reliability. The author has included cooperative, partial-cooperative, and non-cooperative transition states. The reliability of the node depends on the amount of energy dissipated while transmitting and receiving packets. In addition to it, the author has also incorporated link stability based on the mobility of the node. The scheme determines the effective path based on energy level but the involvement of attacks is not contemplated, which results in loss of data packets. Proceeding more, Maragatharajan et al. [6] recommend a Position-based opportunistic (POR) and greedy routing scheme for reliable data delivery. The work adopts a dual-step process to find the best routing path. In the first step, geographic location service (GLS) [7] and Quorum-Based Location Service (QBLS) are incorporated for route discovery; which yields efficient data transmission rate. In the second step, the behavior of nodes in the selected route is derived using the semi-markov process. The scheme approximates the network survivability but quantitative estimation of transition probability is vague and uncertain.

Further, considering node-state transition time as a random variable, Peng et al.[8] incorporated a discrete-time markov chain (DTMC) process for analyzing the behavior of the node. This mechanism addresses the problem of SMS/MMS based worms of smartphone applications through social media. The node is categorized into susceptible, exposed, infectious, and recovered state. The authors have included real-world data set of cellular networks for estimating effective node behavior. The proposed scheme set forth a good detection rate but is specific only to smartphone applications.

Considering the network survivability Sengathin et al. [9] have proposed a futuristic trust coefficient-based semi-markov prediction model (FTCSPM) for mitigating selfish nodes from the compromised network. The model incorporates a non-birth-death process to estimate the trust coefficient. It consists of three state models viz, cooperative, selfish, and failed state. The stochastic transition probabilities estimate the selfish behavior of the node. The model also frames the lower and upper bound of network survivability. The model incorporates only the selfish behavior of the node and lacks to mitigate the malicious activity from the network irrespective of selfishness.

Sometimes the state of the system is unseen and the observer only has certain shreds of evidence to realize the current state. At that instant, the Hidden Markov Model (HMM) comes into play. Liu and Datta [10] proposed an HMM-based context-aware trust model to envisage the dynamic behavior of the agent. In this paper, the authors incorporated entropy-based information theory and multiple key factors for the selection of useful features that defines a complete profile agent. The profile details make for the observation matrix and the quality rating of the agent account for the hidden state. The behavioral analysis of the agent is exploited by finite-state HMM. The proposed mechanism is better than traditional HMM but is specific to agent-based systems and needs to include the effect of malicious attacks.

Heading towards the attack, Pathak et al.[11] proposed an intrusion detection system where they have applied two states' HMM to evaluate the reputation of vehicles. Safe and malicious are considered as a state while send, drop, and forward are regarded as observation states. The authors have directly applied the random probabilities value and have evaluated the reputation of the vehicle. Extraction of these probabilities and derivation of reputation is not discussed. Progressing, Chen et al. [12] proposed a State-based classification model that recognizes multi-stage advanced attacks. The proposed model contains the log of observed activities. Common activities in the log are correlated within a given timeframe into a single event with weight and hit count. The authors have incorporated an

adaptive sliding window approach to correlate the data set. The correlated log accounts for the node's behavior that is examined by the HMM-based model comprising of three stages namely, reconnaissance, attack, and stepping stone. The proposed mechanism yields good detection performance but demands heavy storage space and is limited to IP-address attacks.

Further, Wu et al. [13] proposed an opportunistic data forwarding mechanism (OADM) for the analysis of the node's behavior. The attacking probability of the node is judged by four parameters viz, forwarding rate, residual energy, degree of maliciousness, and state history of the node. These parameters are employed in HMM to yield the current state of the node. For the survivability of the network, an effective relay node is selected to route the packet from source to destination. The mechanism is solitary suitable for on-off attacks.

For multi-stage attacks, Li et al. [14] have proposed a probabilistic intrusion detection system for recognizing malicious events. The work adopts a three-step process for the detection of malicious attacks. In the first step, the temporal relationship is established using HMM between attack phases and intent states. This step measures the deviation of a compromised node from one state to another. Sometimes, the availability of information is incomplete and unidentified, therefore in the next step; a rule-based technique is applied to adjust the parameters at runtime. Finally, to interpret the result Loopy Belief Propagation (LBP) is modeled to optimize the HMM into a single output. The model is acceptable for recognizing the cause-and-effect relationship of known planned attack events. But for unknown attacks, the effectiveness of the model is not good. In addition, the cooperation of nodes in the network is not justified.

Further, Ingale et al. [15] proposed a prediction mechanism using the KDDCUP'99 network intrusion data set. The authors have incorporated both HMM and Naïve Bayes methods for predicting MSA. Though the hybrid form of this model predicts attacks accurately, the redundancy in the KDDCUP'99 dataset results in end-to-end delay.

Out of the literature survey, we could not found any standard mathematical model that successfully incorporates the effect of attacks in a compromised network. Moreover, they demand heavy storage space that affects the residual power of the node, which is not suitable for resource constraint IoT networks. In addition, the survivability and integrity of the network have not been investigated. The comparative analysis of these states of art for hidden markov based trust models are presented in table 1.

Table 1: Comparative analysis of various trust schemes

Trust Model	**Key Target**	**Methodology used**	**Attacks defended**	**Limitations**
FUCEM [5]	To establish effective routing path	Semi-markov approach	None	Lacks to incorporate effect of attacks
POR[6]	Network survivability with effective routing path	GLS, QBLS, semi-markov process	None	Quantitative estimation of transition probability is vague and uncertain.
DTMC[8]	To analyze the behavior of node	Semi-markov approach	SMS/MMS based worms	Specific to only smart phone applications
FTCSPM[9]	To mitigate selfish node from network	Non-birth death process	none	Lacks to mitigate the malicious activity from network irrespective of selfishness
OADM [13]	Analysis of node's behavior	HMM	On-off attack	Fixed for on-off attack
[10]	To investigate the behavior of the agent.	HMM model with entropy-based information system	none	Lacks to show the effect of uncooperativeness.

[12]	To tackle the multistage advance attacks	HMM, Adaptive sliding window approach with log maintenance.	IP address attacks	Demands heavy storage space
[14]	To recognize the malicious events	HMM rule-based technique , Loopy Belief propagation	Recognize known planned attacks	Not good for unknown attacks.
HMT (proposed approach)	To increase the survivability of the network by intelligently mitigating selfish and malicious nodes when it is at the edge of trespassing the network	HMM with the maximum likelihood function	Sinkhole, Blackhole and Grey Hole attacks	Can extend the model by including more observable symbols like degree connectivity and validity can be further improved by modeling against generalized attacks. Besides , other routing protocol like RPL can be included in HMT model for further study.

Further, FUCEM [5], FTCSPM [9], and OADM [13] discussed above are considered for comparison since they are proven as significant models for efficient and effective evaluation of node's trust. In addition, these models predict the node's behavior effectively and improve the performance of the network.

3. System Model

The purpose of the work is to implement the reliable routing path from source to destination along with high network lifetime. The section comprises of network structure and the system architecture of the proposed Hidden Markov Trust Model.

3.1 Network Structure

Here we consider a network incorporated by a set of randomly deployed sensor nodes SN, where 'N' is the number of sensor nodes. Let there be nodes of one of the kinds either adaptive node, mischievous node, or greedy node as shown in figure 1. An optimal trusted path is established between source and destination using LOADng protocol. Consistently, after every time 'T', the behavior of nodes in the path is self quantified through likelihood function (section 4) and are judged as adaptive, malicious, or greedy nodes. The model provides Time-to-Reset (TTR) to the mischievous nodes to improve themselves before withdrawing it from the network routing path. Till that duration, they are allowed to participate and serve the network. The maximum TTR provided is till the trust value outweighs the threshold trust. Thus the involuntary benefit of the malicious nodes taking part in network function can be contemplated and we can exploit the node to improve the survivability of the network till the benefits outweigh the damage to the network. While on the contrary, the selfish nodes whose objective function is to drop the packets are immediately isolated and destroyed from the network as they tend to never participate in the network function. Thus, it's clearly a waste of resources of other nodes to which they attempt to communicate [16]. Eventually, the new trusted routing path free from greedy node and mischievous (when TTR expires) node is established between source and destination.

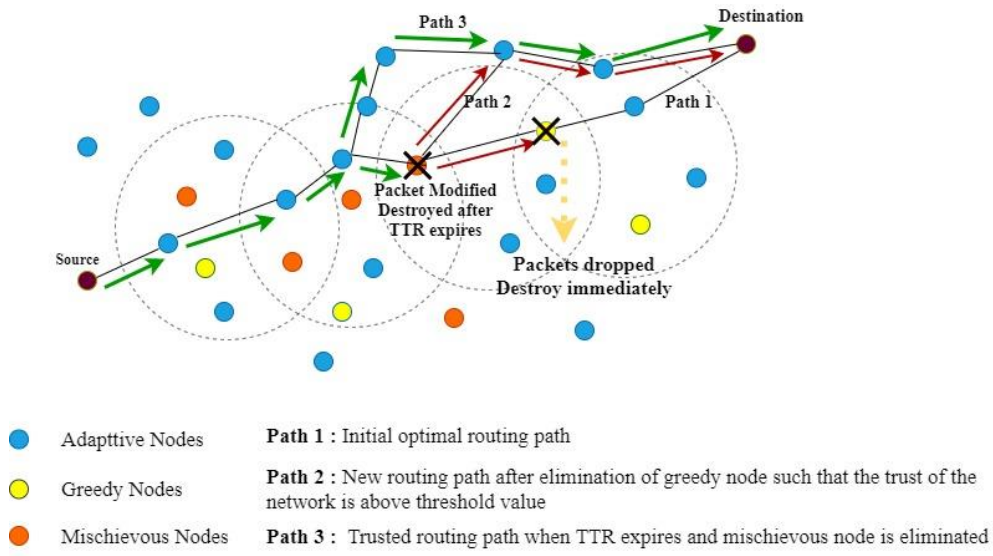


Fig.1 Network Structure

3.2 System Architecture

The proposed system is made up of three modules viz. Path formation module, Learning module, and Decision module (Figure 2). The path formation module evaluates the secured shortest path 'P' to the destination by electing the trustworthy nodes present in the network and initiates the flow of packets. After every time 'T' we train the nodes in the path 'P' using the proposed HMT model and then analyze the behavior of each node. Once the behavior of nodes is examined, the decision module is activated, which eliminates the unreliable nodes from the network. The upcoming section covers the learning and decision module thoroughly while the path formation module is omitted since the optimal path is established using LOADng routing protocol with trust value as an additional attribute.

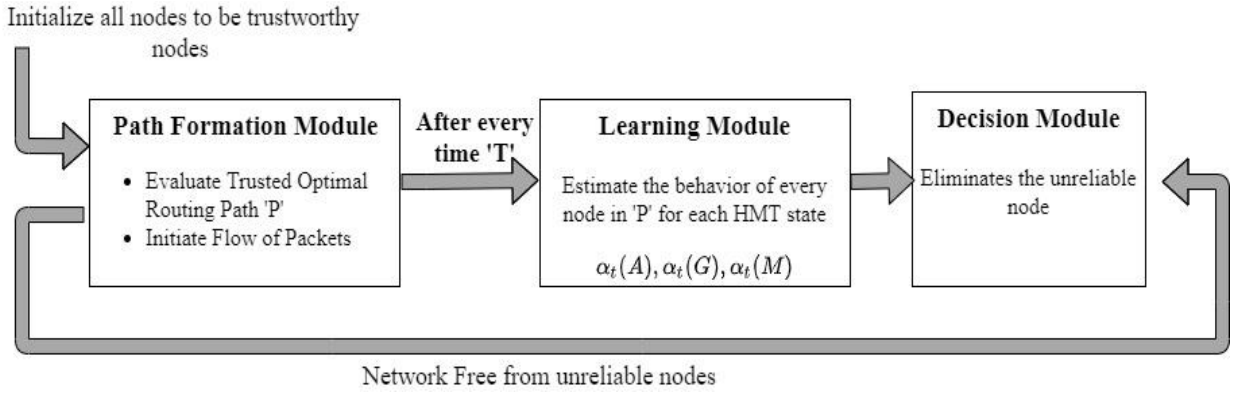


Fig. 2 System Architecture

4. Learning Module: Node Behavior Modeling

The objective of our model is to recognize the reliable movement of packets from source to destination via intermediate nodes. But since the actual state of the node in an IoT network cannot be directly observed, therefore the proposed model had made use of the Hidden Markov process. This is done to observe the behavior of nodes and their attacking probabilities. The probability distribution of the node's state is estimated using the input given and the emitted product visible to the observer. The section covers the basics of HMM and the approach used in our model to estimate the behavior of the node.

4.1 Hidden Markov Model: The Basics

Briefly, HMM [17] is defined as a Quin Tuple Ħ = (Q, O, π, T, E). Where,

Q => It defines the set of distinct states in the Markov process. $\{q_1, q_2, q_3....q_n\}$, where 'n' is the number of states.

O => It is the set of observation symbols. $\{O_1, O_2, O_3.... O_m\}$, where 'm' is the number of observations.

π => It is defined as the initial state of the node at t = 0.

T => It is the state transition probability matrix of size |Q| X |Q|. Where T_{ij} is the probability of the system moving from state q_i at the time't' to state q_j at a time't+1' and $\sum_{j=1}^{n} T_{ij} = 1$

E => It is the emission probability matrix of size |Q| X |O|. Where Ejk is the probability of output O_k at time t when the system is in state q_j at a time 't' and $\sum_{k=1}^{m} E_{jk} = 1$

Provided HMM 'Ħ' and the observations 'O', the likelihood of the system for a given state q_j at time 't'; is estimated by the forward probability algorithm and is expressed as:

$$\alpha_t(j) = \sum_{i=1}^{n} \alpha_{t-1}(i).T_{ij}E_j(O_t), \quad (1)$$

where $\alpha_{t-1}(i)$is the previous forward path probability when the system was at state q_i at previous time step 't-1', T_{ij} is the transition probability from previous state q_i to current state q_j, and $E_j(O_t)$ is the emission probability of the observation O at a time 't' given the current state is q_j.

4.2 Hidden Markov Trust (HMT) Model: the proposed Approach

Greedy and mischievous nodes in the IoT network do not forward the packets properly from one end to another. These nodes drop the packets or tamper the packets, thus are considered as non-cooperative nodes that are not adaptable in an IoT environment.

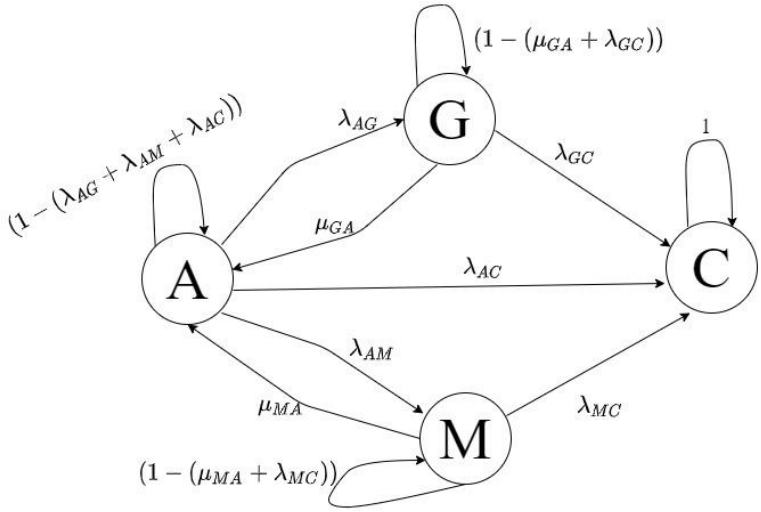


Fig. 3 Transition diagram for the proposed approach

Based on the properties of HMM (section 4.1), the dynamic trustworthiness of the node is modeled by a 4-state HMM model, which predicts the probability distribution of the node's next state. The proposed model is represented as $M_{SI}(N)$ and is defined as quintuple $M_{SI}(N)$ = (S, O, π, P, E) (figure 3), where

'S' is the finite state space that defines the behavior of the node. It consists of four states: adaptive(A), greedy(G), mischievous(M), and crashed(C) state. The adaptive state is also known as the cooperative state; here the node is reliable to forward packets from one end to another. Nodes in a greedy state are selfish in nature, so instead of forwarding the packets of another node, they drop the packets to save their energy. Mischievous (malicious) nodes

restrain the integrity of the data by tampering with the data packets of other nodes while in transmission. Nodes in a crashed state are said to be failed nodes that do not take part in routing.

'O' is the set of emitted symbols; visible to users while there is the transmission of data from source to destination. It consists of two symbols: expected output (EO) and unexpected output (UEO) at each state.

'π' is the initial state probability of the node at time 't =0'. When the network is deployed all nodes are assumed to be adaptive in nature i.e., π = {1,0,0,0}

'P' is expressed as state transition probability of matrix of size 4 x 4. (section 4.3)

'E' is expressed as the emission probability matrix of size 4 x 2. (Section 4.4)

Estimation of stochastic probabilities 'P and 'E' are discussed in upcoming sections.

4.3 Estimation of state transition probabilities (P)

The state transition probability matrix provides the probability of a node transitioning from one state to another in a single time unit. The transition probabilities of the proposed model are derived from the data flow rate of the packet and the residual energy of the node. As shown in figure 3, the stochastic transition probabilities are classified as:

λ_{AG}=> A cooperative node in an IoT environment begins to enter into the greedy state when the residual energy of the node comes down. The average lifetime of the node defines the probability of it; transiting from adaptive to greedy state. It is determined as the ratio of energy consumed by the node in receiving and transmitting packets to the energy left after interplay.

$$\lambda_{AG} = \frac{E_c}{E_r} = \frac{E_i - E_r}{E_r}, \tag{2}$$

Where,E_c is the energy consumed, E_r is residual energy, E_i is initial energy.

From eq 2, a node is considered to be adaptive when the value of 'λ_{AG}' is less i.e., residual energy of the node is high.

μ_{GA} => A greedy node at times attempts to cooperate and tries to adapt itself in an IoT environment by forwarding data packets on behalf of their neighbor nodes. Thus, the probability of a node to transit its state from greedy to adaptive is the ratio of the number of packets forwarded to the total number of packets received from neighbor nodes.

$$\mu_{GA} = \frac{pkts_f}{pkts_r} \tag{3}$$

Where,$pkts_f$ is the number of packets forwarded,$pkts_r$ is the number of packets received.

$\lambda_{AC} = \lambda_{GC} = \lambda_{MC}$ =>A node in any state tends to enter the crashed state if it starts dropping the packets instead of transmitting them. So, the transition probability of node from any of the states (adaptive, greedy, and mischievous) to crashed state is given as the ratio of the number of packets dropped to the number of packets received by the node.

$$\lambda_{AC} = \lambda_{GC} = \lambda_{MC} = \frac{pkts_d}{pkts_r} \tag{4}$$

Where, $pkts_d$ is the number of packets dropped, $pkts_r$ is the number of packets received.

λ_{AM} =>We assume an attack model that interrupts the integrity of the message forwarded from source to destination. Therefore, the probability of transition from adaptive to mischievous state can be referred to as the ratio of the number of packets modified to the number of packets received by the node (eq 5). Furthermore, to detect which node modifies the packet we have implemented the concept of checkpoint after every 'm' multiple hop. Checkpoint is used to declare the point before which all nodes are in a consistent state and had transmitted unmodified packets. Maintenance of this save point is done by an edge node. After every 'm' hops edge node

verifies the forwarded packets by comparing them with the source data packets. If the packet received is damaged, it will backtrack all nodes one by one, till the previous save point. We rely on the fact that nodes store their data till the next checkpoint is administered. Thereby, the number of packets modified by each node is discovered and the transition probability of node from adaptive state to modified state is evaluated.

$$\lambda_{AM} = \frac{pkts_m}{pkts_r} \tag{5}$$

Where, $pkts_m$ is the number of packets modified (tempered), $pkts_r$ is the number of packets received.

μ_{MA} => It is possible that the mischievous node can be released from the impact of an intruder. So instead of immediately isolating a node, few opportunities can be given to it; to correct itself and get removed from malicious activity. Thus, the rehabilitation probability of the node is given as

$$\mu_{MA} = \frac{1}{TTR} \tag{6}$$

Where Time-to-Reset (TTR) is the time required to realign itself into an adaptive state.

Summarizing, the above transition probabilities, the complete state transition probability matrix is given as in eq 7

$$P = \begin{bmatrix} & Adaptive(A) & Greedy(G) & Mischievous(M) & Crashed(C) \\ Adaptive(A) & (1-(\lambda_{AG}+\lambda_{AM}+\lambda_{AC})) & \lambda_{AG} & \lambda_{AM} & \lambda_{AC} \\ Greedy(G) & \mu_{GA} & (1-(\mu_{GA}+\lambda_{GC})) & 0 & \lambda_{GC} \\ Mischievous(M) & \mu_{MA} & 0 & (1-(\mu_{MA}+\lambda_{MC})) & \lambda_{MC} \\ Crashed(C) & 0 & 0 & 0 & 1 \end{bmatrix} \tag{7}$$

4.4 Estimation of Emission Probability Matrix (E)

Emission probability also termed as observation output probability is defined as the probability of a node to yield each output (observation) symbol from every single state in a single time unit. Given as in eq 8

$$E_{jk} := Probability\left(O_k at\ time\ t \middle| S_j\ at\ time\ t\right) \tag{8}$$

As discussed in section 4.2, the proposed model assumes two observation symbols, which are expected output and unexpected output. So, the emission probability matrix from eq 8 is presented in eq 9:

$$E := \begin{bmatrix} & Expected\ output(EO) & Unexpected\ output(UEO) \\ Adaptive(A) & \frac{No.of\ correct\ pkts\ fwd}{No.of\ pkts\ received} & 1-\frac{No.of\ correct\ pkts\ fwd}{No.of\ pkts\ received} \\ Greedy(G) & \frac{No.of\ pkts\ dropped}{No.of\ pkts\ received} & 1-\frac{No.of\ pkts\ dropped}{No.of\ pkts\ received} \\ Mischievous(M) & \frac{No.of\ tempered\ pkts}{No.of\ pkts\ received} & 1-\frac{No.of\ tempered\ pkts}{No.of\ pkts\ received} \\ Crashed(C) & 0 & 1 \end{bmatrix} \tag{9}$$

4.5 Evaluation of Trusted Node based on Hidden Markov Model (MSI(N))

Provided the model $M_{SI}(N)$ (Section 4), the likelihood of the node with the expected output, to be trusted in the routing process, is estimated using the forward probability algorithm. Utilizing equation 1 we have:

- The probability of a node to be in adaptive state at the time 't' with expected output is given as:

$$\alpha_t(A) = \alpha_{t-1}(A).P_{AA}.E_A(EO_t) + \alpha_{t-1}(G).P_{GA}.E_A(EO_t) + \alpha_{t-1}(M).P_{MA}.E_A(EO_t) + \alpha_{t-1}(C).P_{CA}.E_A(EO_t) \tag{10}$$

- Similarly, the probability of a node to be in a Greedy state with expected output is given as:

$$\alpha_t(G) = \alpha_{t-1}(A).P_{AG}.E_G(EO_t) + \alpha_{t-1}(G).P_{GG}.E_G(EO_t) + \alpha_{t-1}(M).P_{MG}.E_G(EO_t) + \alpha_{t-1}(C).P_{CG}.E_G(EO_t) \tag{11}$$

- The probability of a node to be in a Mischievous state with expected output is given as:

$$\alpha_t(M) = \alpha_{t-1}(A).P_{AM}.E_M(EO_t) + \alpha_{t-1}(G).P_{GM}.E_M(EO_t) + \alpha_{t-1}(M).P_{MM}.E_M(EO_t) + \alpha_{t-1}(C).P_{CM}.E_M(EO_t) \quad (12)$$

4.6 Decision Making Module

The maximum likelihood of the node's behavior determines the isolation of the node and the integrity is maintained by utilizing the likelihood of expected valid output that is regulated at different states. Maximum of $\alpha_t(A)$, $\alpha_t(G)$, and $\alpha_t(M)$ stimulate the state of the node. If the maximum value out of three is $\alpha_t(M)$, then the node is mischievous in nature. It is not immediately isolated but is given TTR time to reset and detach itself from the malicious effect. TTR is selected to such an extent, that benefits to the network always overpower the damage caused. As from eq. 10, it is evident that TTR is inversely proportional to trust. Thus the value of TTR is so forth selected, that the probability of trust is always above its threshold value. This is done to increase the survivability of the network. Secondly, if the maximum value is $\alpha_t(G)$, then the node is said to be greedy in nature. The greediness of the nodes can be due to certain reasons. First, a node can have minimum energy and can be at the edge of the crashed state. In this situation, the node is only isolated from the routing function and is provided Time-to-Live (TTL) to restore its energy. If the node recovers before TTL expires, it is carried back to the network else crashed. Second, a node can be selfish in nature where despite having adequate energy, it intends to never participate in the network function. In such a case, the node is immediately isolated and destroyed from the network. The line of greediness is evaluated by measuring the energy of the greedy node. Finally, if the maximum value is $\alpha_t(A)$, then it determines that the node is trustworthy but besides trustworthiness, if the trust value is more than the trust threshold then the node is adaptive in a network environment with valid output else it yields invalid output because of mischievous activity along the path. Figure 4 illustrates the decision module of the proposed solution.

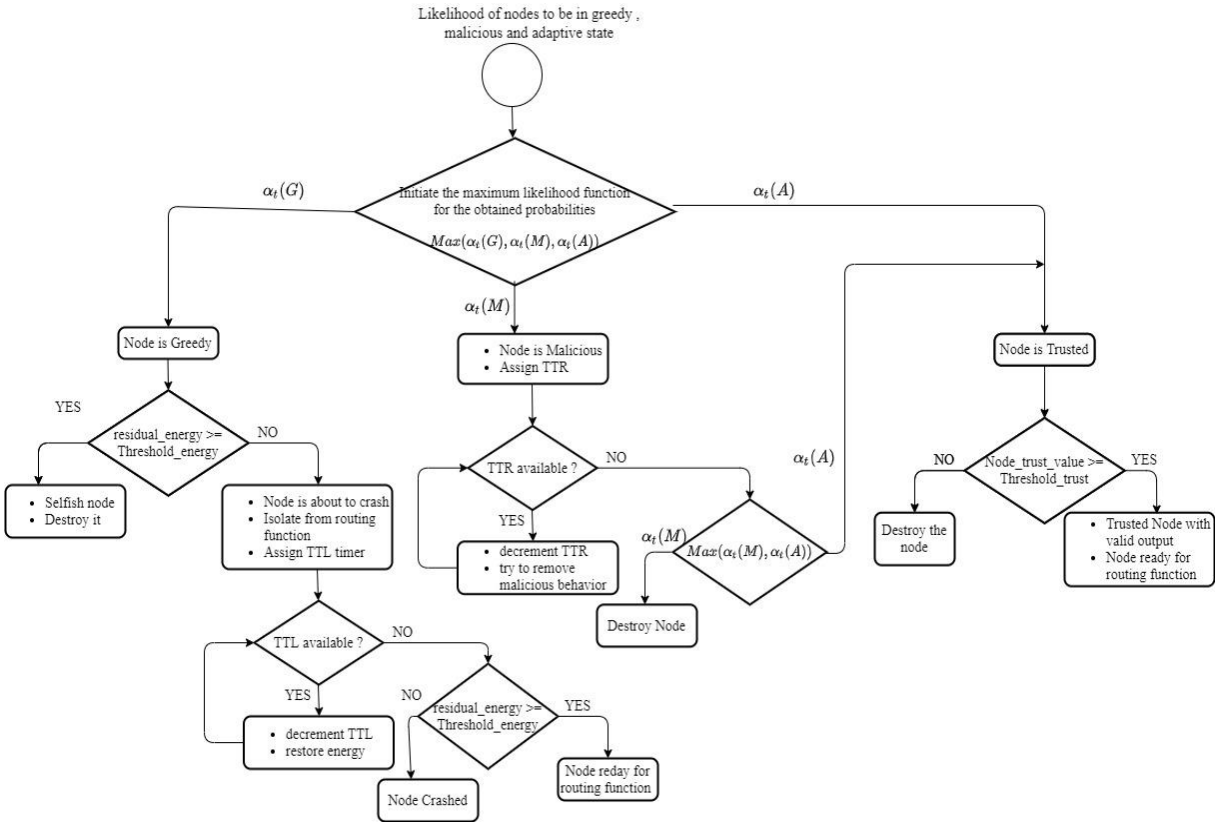


Fig. 4: Decision module of the proposed solution

5. Simulation results and analysis

Till now, we have obtained the probability of node behavior in different states. This section presents the simulation environment and the network survivability of IoT networks.

5.1 Simulation Environment

In this work, we use MATLAB-R2018 to perform the simulations. All simulations are performed in a 500 X 500 m^2 approximately; over 50 nodes with a transmission range of 150 m are distributed randomly since it generates a realistic node pattern. The traffic of the simulated model is represented in terms of a constant bit rate with 40 pkts/sec. Further, modified LOADng is used as a routing protocol and the simulation time is set to 400 sec. Table2 presents the simulation parameters for analyzing network performance.

TABLE 2: Simulation Configuration

Simulation Parameters	Values
Maximum Number of nodes	50
Protocol	LOADng
Initial energy	10 J
Energy threshold	4 J
TTL & TTR	2sec
Percentage of unauthenticated nodes	5%
Maximum number of compromised nodes	5
Area Size	500 m^2 x 500 m^2
Packet Size	500 bytes
CBR	40
Range	150 m
Time interval for path selection(T)	15 sec
Time for simulation	400 sec

Initially, all nodes in the network are adaptive in nature and the modified LOADng routing path is selected for traffic movement from the source to the gateway. Once the trusted path is selected, traffic continues to move from source to gateway for 'T' sec. After every 'T' sec, the path is analyzed again, mistrusted nodes are isolated and a new reliable trusted path is selected for traffic movement. This continues until the end of the simulation. We tested our proposed solution on a varied number of nodes and attack percentages and classified this into different cases. Case I deals with the simulation of a Blackhole attack with different network sizes and vulnerabilities. Case II hands out a simulation of a Greyhole attack with varying network size and vulnerability and Case III presents the sinkhole attack in a scalable and vulnerable environment.

In addition, the survivability of the network depends on the behavior of the node towards the establishment of a reliable routing path [18], [19]. However, the presence of selfish and malicious behavior drastically influences the survivability, integrity, and throughput of the network. Hence the performance of the model; is evaluated based on the following parameters such as survivability rate, packet delivery ratio, average energy consumption, average end-to-end delay, routing overhead, detection rate, average trust value , false-positive, and false-negative rates.

- *Survivability rate*– It is defined as the capability of the system to fulfill its objective in a timely manner, in the presence of attacks, failures, or accidents. It is the ratio between the number of active nodes and a total number of nodes present in the network at a particular instant.

$$Suviability\ rate = \frac{N_{active}}{N}, \tag{13}$$

  where N_{active} is the number of active nodes in the network and N is the total number of nodes.
- *Packet Delivery Ratio (PDR*) – It is the ratio of the number of packets received by the destination node to the number of packets sent to the destination node.

$$PDR = \frac{number\ of\ packets\ received}{number\ of\ packets\ sent} \tag{14}$$

- *Routing Overhead*–It is considered as the frequency of discovering routing paths.

$$Routing\ Overhead = \frac{Number\ of\ routing\ packets\ for\ route\ dicovery\ and\ maintenance}{Total\ number\ of\ received\ packets} \quad (15)$$

- *Detection Rate*–It is the amount of malicious or selfish nodes detected from the pool of nodes in a network.

$$Detection\ rate = \frac{Number\ of\ attacking\ nodes\ detected}{Total\ number\ of\ attacking\ nodes} \quad (16)$$

- *False positive rate* –It is the ratio of number of false positive to the total number of negative events.

$$FPR = \frac{FP}{FP+TN} \quad (17)$$

where FP is number of negative events wrongly categorized as positive, TN is is the number of true negative events.

- *False negative rate* – It is the ratio of false negative to the total number of positive events

$$FNR = \frac{FN}{FN+TP} \quad (18)$$

where FN is number of false negatives, TP is is the number of true positive events.

- *Avg Energy Consumption* – It is the total energy consumed by the node during the packet transmission and reception.
- *Avg End-to-end Delay* – It is the average time taken by the data packets to reach their destination along with connection establishment and delays.
- *Average Trust value* – Trust is defined as an association between two nodes. Average trust is the degree of node to be collaborative in nature.

5.2 Impact of TTR on the survivability of the network

The section analyses the effect of TTR on the survivability and overall trust of the network. Figure 5(a) compares the survivability rate against time for TTR = 0, 1, 2 and 3 sec. We observe that the survivability rate of the network decreases abruptly with lower values of TTR. The model estimates on an average 93.2% of survivability for TTR = 3sec, which is then dropped to 91.6 % for TTR = 2sec followed by 89.6% and 73.6 % for TTR = 1sec and TTR = 0 respectively. On contrary, Figure 5(b) compares overall trust against time for the same values of TTR. We observe that the trust value decreases gradually with an increase in TTR. The model estimates the probability of trust to be 0.95 when no time-based opportunity is given (i.e. TTR = 0) to nodes. Trust value reduces by 4%, 1% and 0.5 % for TTR = 1, 2 and 3sec respectively. Comparative study of figure 5(a) and figure 5(b) states though time-based opportunity (TTR) decreases the overall trust; but when benefits (survivability) are analyzed, the model outperforms and gives a better result. Therefore, the value of TTR has to be opted to an extent that trust value does not drop below threshold trust. Thus we can infer that providing a time-based opportunity to nodes in the network plays an important role in the welfare of IoT network communication. In addition, both figure 5(a) and 5(b) presents the decrease in survivability rate and trust value as time proceeds. This is because with time residual energy of the nodes becomes less.

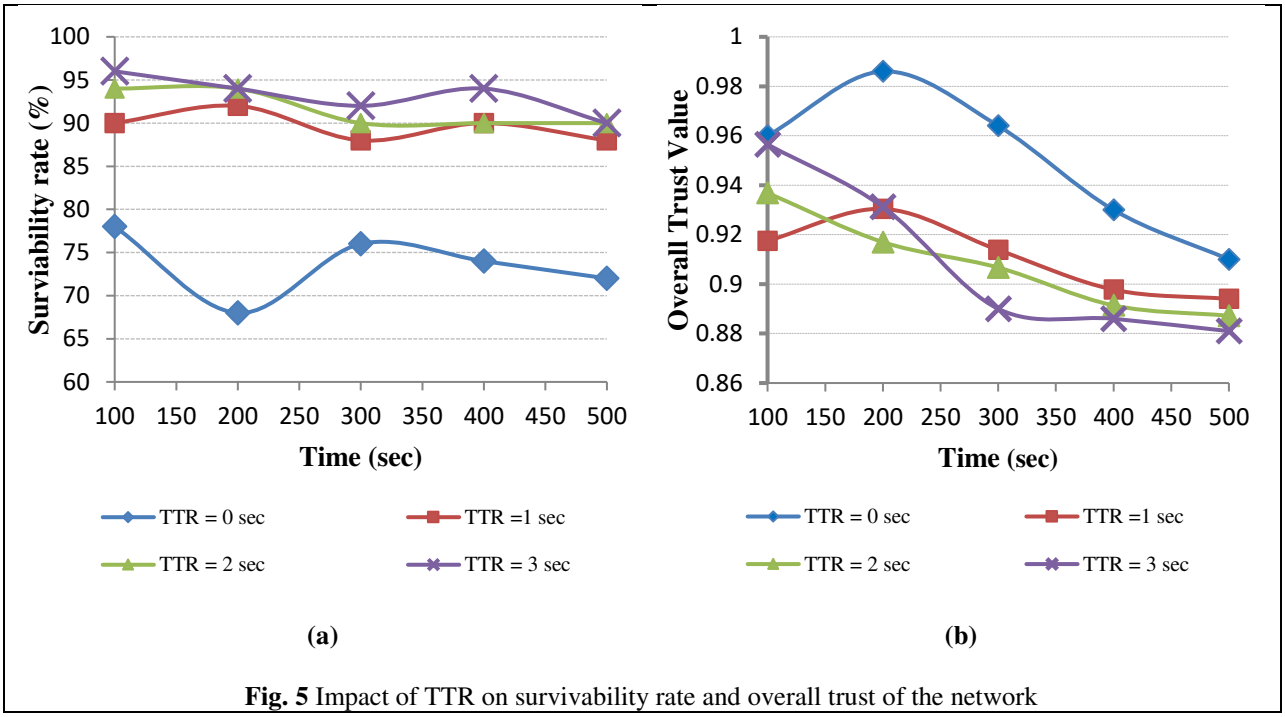


Fig. 5 Impact of TTR on survivability rate and overall trust of the network

5.3 Performance of the model in presence of various attacks

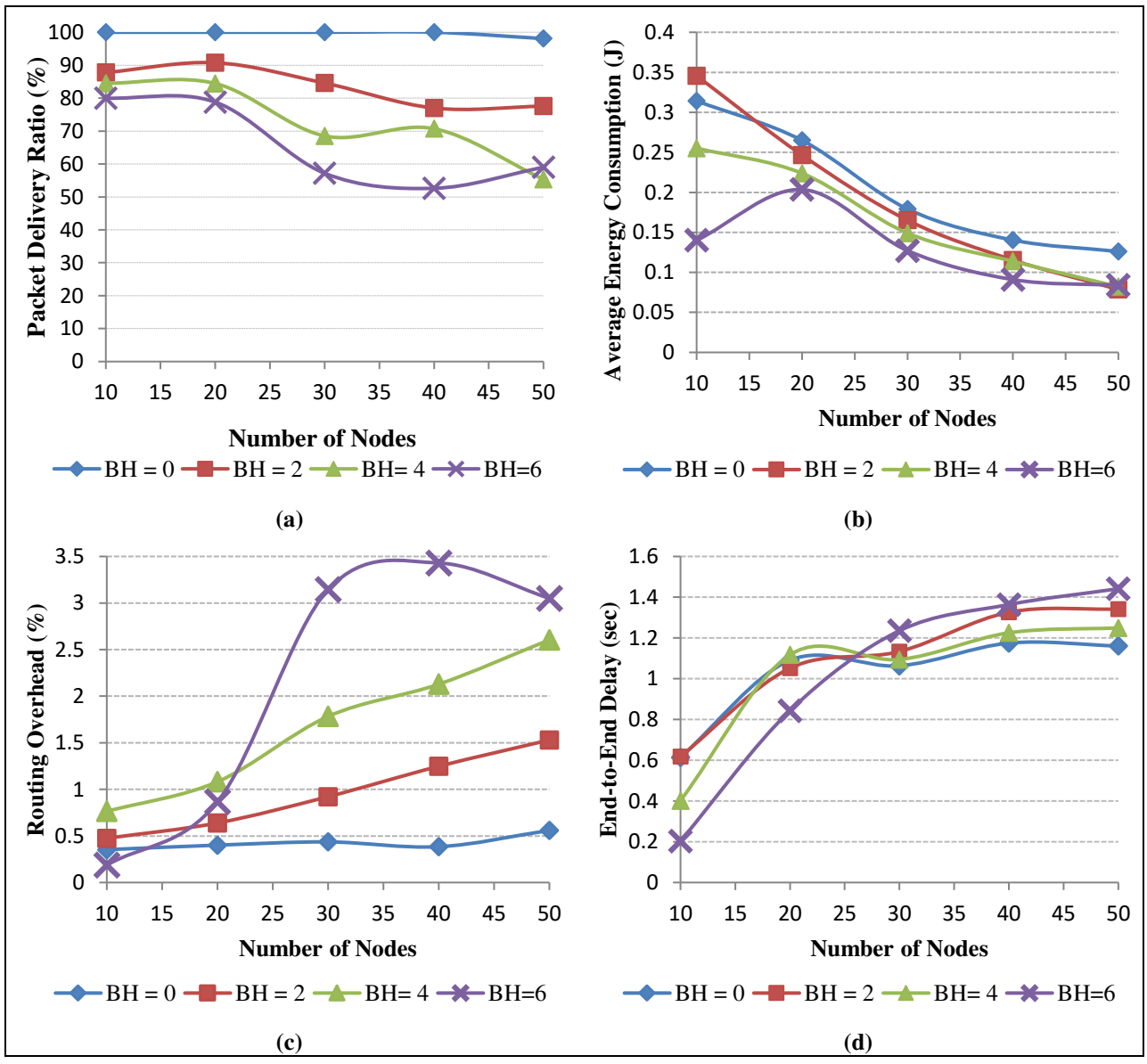
In this section, the impact of Blackhole (BH), Greyhole(GH), and Sinkhole(SH) attacks in IoT networks is been examined for different performance parameters as discussed in section 5.1. A blackhole (BH) attack is an attack where the attacker claims that it has the shortest route to the destination node, even if it does not have any route to it. Consequently, all packets pass through it and this enables the attacker node (BH node) to forward or discard packets during the data transmission. Further, a Greyhole attack is a variant of a BH attack, where GH nodes drop the packets with a certain probability. These nodes discard packets for some particular time duration and then switch back to normal behavior, resulting in on-off vulnerability. And Sinkhole attack is the type of attack where compromised nodes launch other types of attacks like GH and modification attacks. During the course of action, it aims to drop or modify the data information, thereby making its detection even more difficult. Different test scenarios for the proposed solutions are:

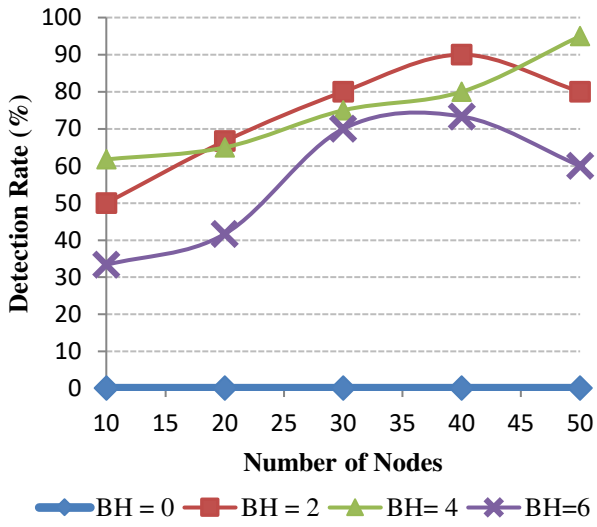
Case I: Simulation of Blackhole attack with different network size and adversary

Simulation is carried out in presence of various BH nodes from sparse (10 nodes) to dense (50 nodes) sensor network. The comparisons were made for a different number of blackhole nodes (BH=0, BH=2, BH=4, BH=6). The performance of the network is depicted in Figure 6(a – e) and the following observations are drawn:

1) As shown in figure 6(a), the result of PDR in the absence of BH node (BH=0) is highest irrespective of the number of sensor nodes in the network. The plot depicts a decrease in PDR by 18%, 45%, and 75% for BH=2, BH=4, and BH= 6 respectively, when the network is neither sparse nor dense (30 nodes). This is because the BH node in the network aims to cut the connection between two communicating nodes and absorb all intercepting packets. Looking at the results, when the network progresses from sparse to dense, PDR decreases due to the collision of packets during data transmission.
2) Figure 6(b), depicts the average energy consumption of the nodes in presence of BH nodes. The model reveals the highest energy consumption in absence of BH nodes, but as the BH nodes increase energy consumed by nodes is decreased by 8%, 20%, and 40 % for BH= 2, BH= 4, and BH= 6 respectively because packets are dropped by attacking nodes. Therefore, normal nodes tend to remain ideal as they have no forwarding packets. In addition, our proposed solution serves to distribute energy among mobile nodes. Consequently, an increase in mobile nodes decreases the energy consumption which is evident from the graph.

3) Figure 6(c) illustrates the routing overhead of the model in presence of BH nodes. Isolating BH (selfish) nodes from the network initiate the selection of a new routing path from source to destination. Routing overhead is high for a large number of BH nodes and low in absence of it, as the transmission of all packets takes place in a single run. The overhead is increased by 86% for BH=6 when compared to the network without BH nodes. Moreover, the number of mobile nodes also increases the routing overhead because more control packets are required to discover the routes.
4) Figure 6(d) presents the result of end-to-end delay with varying network sizes and BH nodes. Initially, in a sparse network, the result of delivering packets from source to destination is low, but as the network size increases, the transmission speed from source to destination becomes less resulting in a 47% increase in end-to-end delay. Since the packets have to hop through an extra number of nodes. Likewise, the increase in BH nodes also increases the delay, as the compromised nodes restrict the data transmission resulting in the resending of the packets.
5) Figure 6(e) depicts the detection rate of the compromised nodes. It is inferred, the quantity of nodes in the network helps in increasing the detection rate on an average by 60%. Besides this, on the contrary, attackers try to reduce the rate of detection within a specified network size. It is observed, when BH=6, then approximately 60% of the BH nodes are detected while when BH=4, 75% of the BH nodes are discovered. In addition, the position of BH nodes plays an important role, if the location is close to the network traffic then compromised nodes can be easily detected compared to a node located at a distance.





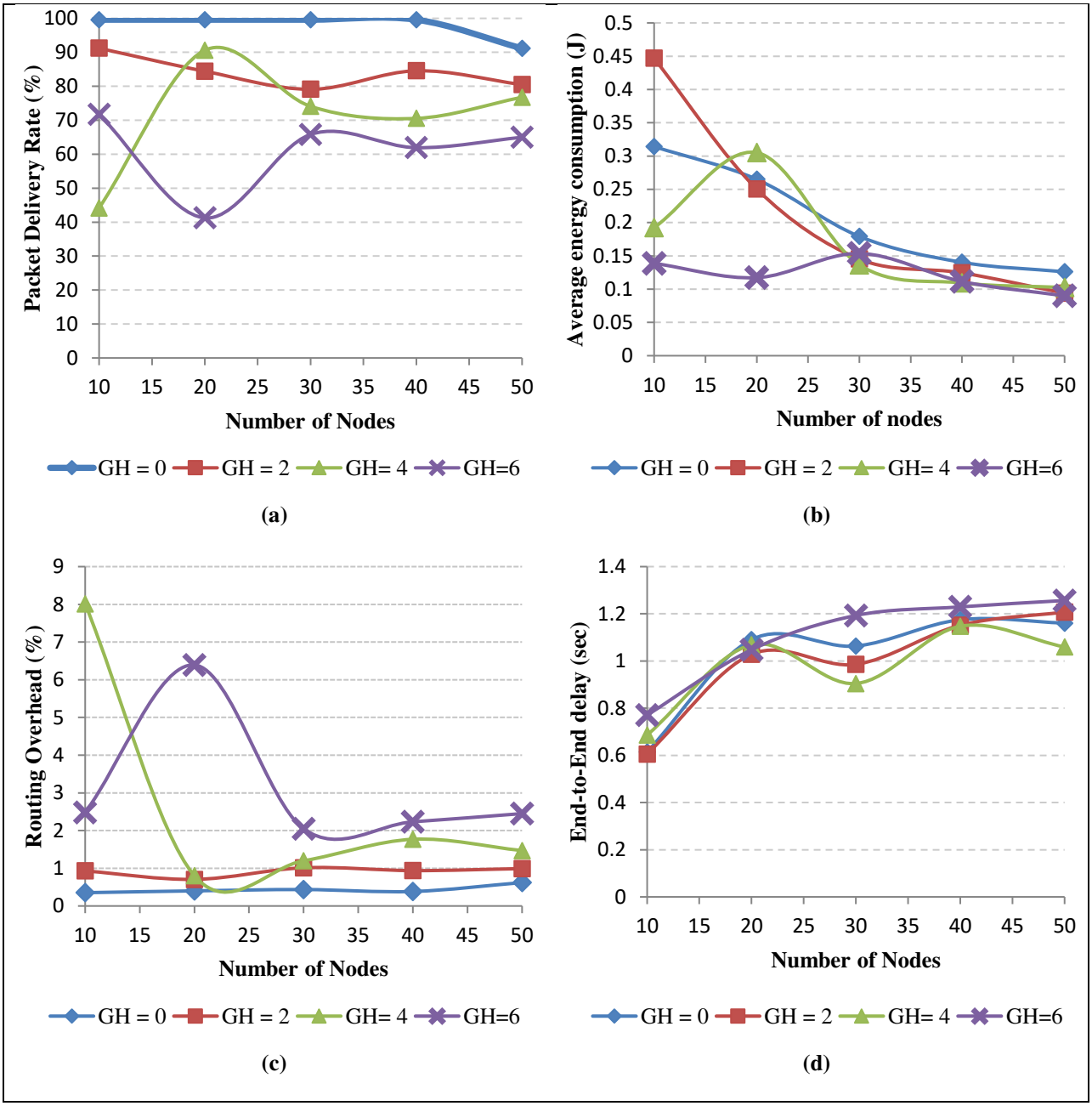
(e)

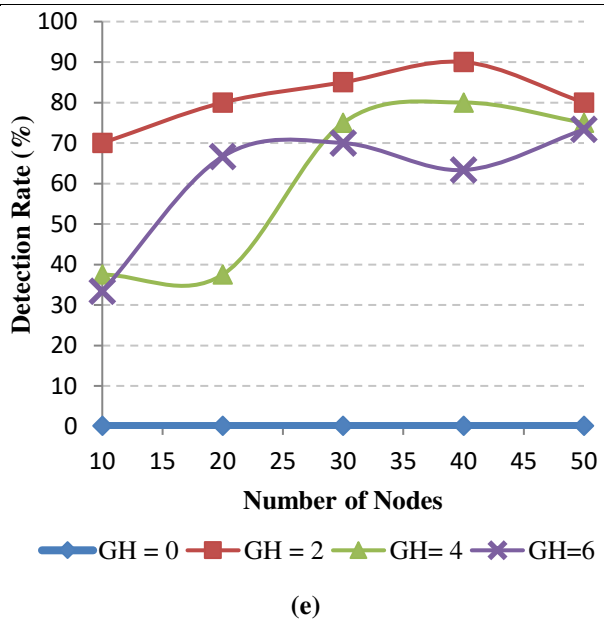
Fig. 6 Performance metrics of the proposed approach for IoT network in presence of Blackhole attack

Case II: Simulation of Greyhole attack with different network size and adversary

The section discusses the impact of GH attacks on IoT networks. We have analyzed and demonstrated the discussed performance metrics. The following observations are drawn:

1. Figure 7(a) demonstrates that the effectiveness of GH nodes on sensor networks is similar to existing BH effects. Observation states that PDR decreases with an increase in the number of mobile nodes due to collision and with the increase in GH nodes, which aims to absorb all the forwarding packets. The average decrease in PDR is 37% when the number of GH nodes is six with respect to the network without any GH nodes. However, the impact of GH nodes in PDR is approximately 5% higher than BH nodes. This is because; GH nodes switch their behavior after every specified time. This allows the partial flow of packets.
2. Figure 7(b), illustrates the decrease in average energy consumption of the nodes with the increase in the number of mobile and GH nodes. On average, energy consumption is reduced to 67%, when GH= 6 with respect to network free from GH attack. Energy consumed by GH attackers is 10% more than BH attackers in sparse networks followed by a 12% increase in the dense network since the switching nature of GH nodes manages to forward some packets.
3. Figure 7(c); represent the routing overhead in the presence of GH nodes. Initially routing overhead is low for GH = 0, and GH = 2 but as the network becomes dense routing overhead increases and becomes stable because the selection probability of trusted path is more than un-trusted path. While on the contrary rise in GH nodes, escalates the routing overhead of the network because every time the selection of a new routing path is initiated. The graph depicts 0.6 % and 0.8 % of overhead when GH=2 and GH=4, which instantly increase to 6.8 % when GH= 6, because each time the new path is initiated which increases the flow of control packets.
4. Delay in delivering packets from source to destination is highlighted in figure 7(d). On average packet is delayed by 1sec in absence of GH nodes and then as the attacking likelihood increases delay to 1.3 sec. The graph shows small variations because the on-off nature of GH nodes models them to be equivalent to normal nodes. Besides, due to the same reason, the overall delay in presence of GH nodes is less when compared to BH nodes. In addition, the delay is increased with increasing mobile nodes because packets now have to cover more hops.
5. Attack detection analysis in figure 7(e) depicts the unstable rate of detection because the position and on-off nature of the GH node play a key role in the detection mechanism. Moreover, the average detection rate of BH nodes is 2% higher than that of GH nodes because the unpredicted nature of GH nodes helps them to cover up themselves in the normal nodes, thereby making detection difficult.


Packet Delivery Rate (%)
Number of Nodes
GH = 0
GH = 2
GH= 4
GH=6
(a)
Average energy consumption (J)
Number of nodes
GH = 0
GH = 2
GH= 4
GH=6
(b)
Routing Overhead (%)
Number of Nodes
GH = 0
GH = 2
GH= 4
GH=6
(c)
End-to-End delay (sec)
Number of Nodes
GH = 0
GH = 2
GH= 4
GH=6
(d)



(e)

Fig. 7 Performance metrics of the proposed approach for IoT network in presence of Greyhole attack

Case III: Simulation of Sinkhole attack with different network size and adversary

A sinkhole attack is a generalized attack that includes the previously discussed attacks along with a modification attack. This attack is investigated by various researchers; therefore a comparative analysis with other models like FTCSPM [9], FUCEM [5], and OADM [13] is presented in this section.

a) Performance metrics versus varying number of mobile nodes

We present the performance of the proposed approach by differing the number of mobile nodes in the environment. The number of nodes is varied from 10 to 50 with 10% nodes as misbehaving nodes. Fig 8a – d depicts the plots of average energy consumptions, packet delivery ratio, average delay, and routing overhead for our approach along with comparative models.

1) The plot depicted in figure 8(a) shows the node's average energy consumption of the proposed approach with the three discussed benchmark systems. It can be illustrated that in general, energy consumption considerably increases when the number of mobile nodes in the network increases; this is due to the increase in the data flow. But the proposed approach consumes less energy as compared to others when mobile nodes in the environment are multiplied. This is due to the effectiveness of our approach which despite the huge data flow distributes the energy among the varying mobile nodes during the period of transmission. Since energy consumption depends on the distance between the two nodes. Though the proposed approach initially shows an increase of 0.1J, 0.09J, and 0.121 J when compared with FTCSPM, FUCEM, and OADM respectively. But as the mobile nodes increases, the proposed approach shows a considerable decrease in energy consumption with 0.03 J, 0.88 J, and 0.32 J with 50 nodes when compared with FTCSPM, FUCEM and OADM respectively.
2) The plot in figure 8(b) presents the PDR of the proposed approach with three benchmark mechanisms. The figure concludes an increase in PDR from 17% to 30% with respect to FTCSPM, from 3% to 12% with respect to FUCEM, and 0.5% to 1.5% with respect to OADM. All in all, the proposed approach shows a significant improvement in PDR by 10.5%.
3) Further, figure 8(c) plots the average end-to-end delay for the given number of mobile nodes. The graph depicts, a significant decrease in average delay because only the reliable routing path is selected which prevents unnecessary delay. On average the proposed approach presents 90%,62%, and 13% decrease in delay when compared to FTCSPM, FUCEM, and OADM respectively.
4) Finally, figure 8(d) depicts the plot of routing overhead derived for a different number of mobile nodes. The figure presents the increase in overhead with the increment of nodes. It can be concluded that our model shows a significant increase in performance by an average decrement of 88%, 92%, and 56.6% of overhead for

FTCSPM, FUCEM, and OADM respectively. This is due to the adopted strategy which selects the routing path with the minimal number of control packets.

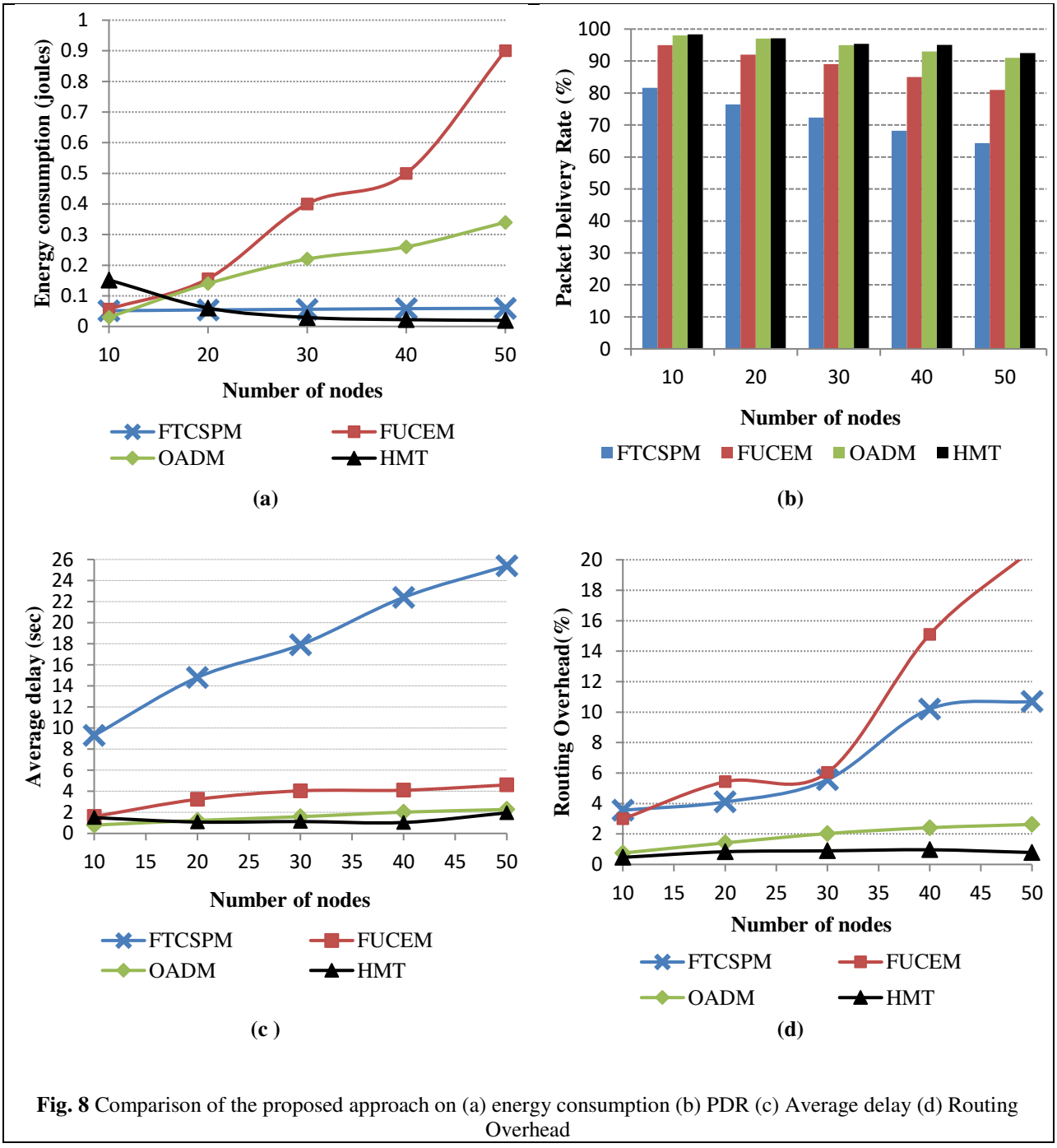


Fig. 8 Comparison of the proposed approach on (a) energy consumption (b) PDR (c) Average delay (d) Routing Overhead

b) Performance metrics versus varying number of attacking nodes

Here the performance of the proposed approach by varying the number of attackers in an IoT environment is explored. The percentage of attackers is varied from 10% to 50% with a total of 50 IoT nodes. Fig. 9(a) – 9(c) depicts the plot of PDR, routing overhead, and detection rate in presence of floating attackers. The plots are compared with FUCEM [5] and OADM [13]. Here we have not used FTCSPM [9] for comparative measurement because the model deals only with selfish activity, the effect of maliciousness is not included.

1) The plot depicted in figure 9(a) shows that there is a decrease in PDR with an increase in the percentage of attackers for all the included benchmarks. However, the proposed approach shows considerable improvement in PDR when compared to other mechanisms. The proposed model on average shows an 8% increase when compared to OADM and a 0.7% increase when compared to FUCEM. All in all, the proposed approach presents a significant improvement because the most reliable and shortest path is selected that allows the significant flow of packets.
2) Further, the plots depicted in figure 9(b) shows routing overhead with varying amount of attackers. Plot infers that injection of attackers escalates the routing overhead. However, our approach presents a lesser increment in routing overhead. On average, our approach is 76% better than OADM and 29% better than FUCEM. On the whole, our approach is superior because the most trusted routing path is selected whereas in other cases some misbehaving nodes are misjudged as collaborating nodes. This results in frequent discovery of paths, ending up with overhead augmentation.
3) Finally, the plot in figure 9(c) depicts the detection rate of misbehaving nodes. It can be inferred that attackers decrease the detection rate. According to the plots, our approach is stronger than other benchmarks. Relatively, our approach recognizes attackers 5.4% more than OADM and 1.5% more than FUCEM. This is because the observable symbols in the HMM model immediately identify the state of the node.

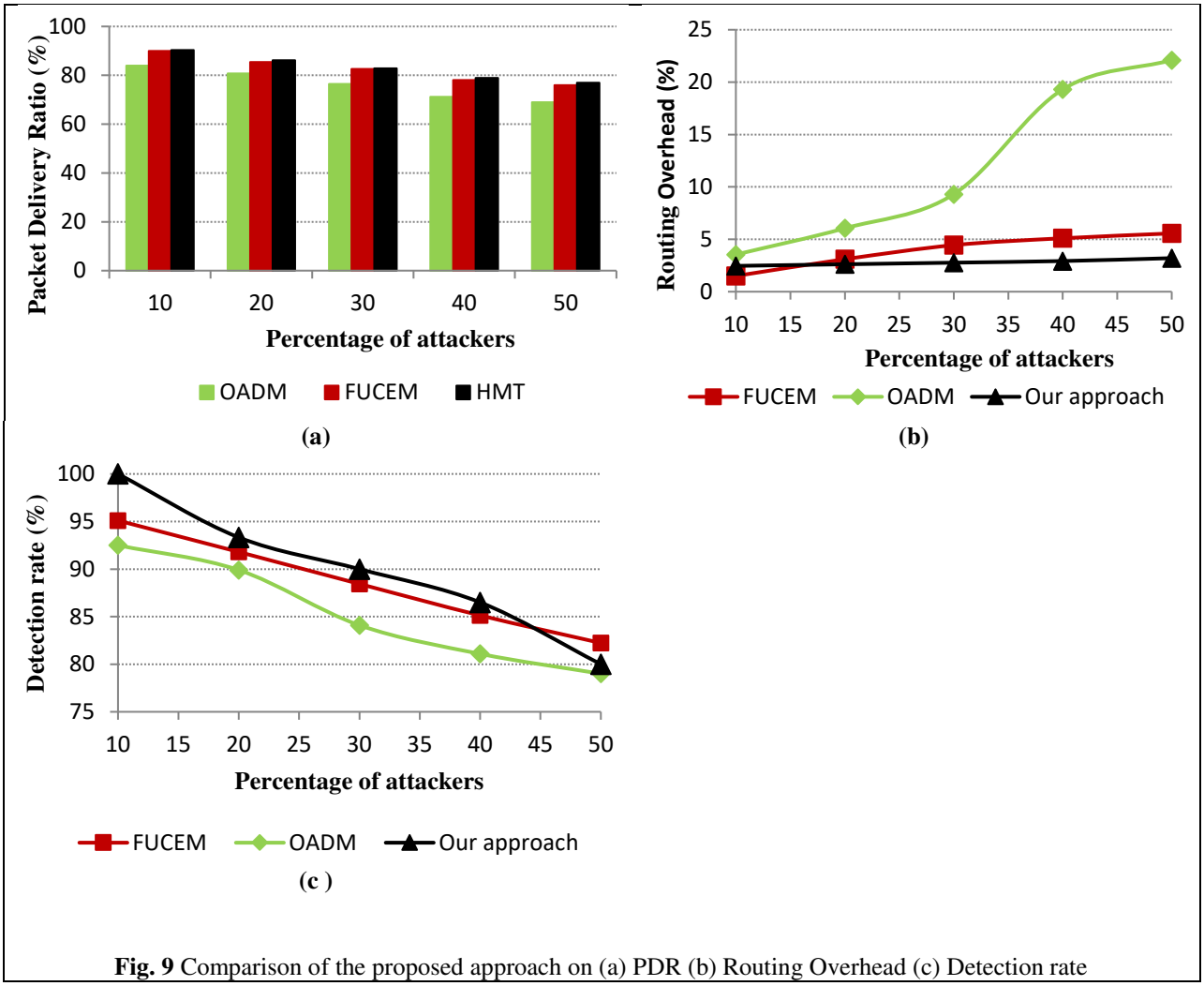


Fig. 9 Comparison of the proposed approach on (a) PDR (b) Routing Overhead (c) Detection rate

5.4 False alarm probabilities and the accuracy of the model

This section states the rate of false-positive and false-negative along with the accuracy of the proposed solution in presence of 50 nodes with 5 compromised nodes. Figure 10(a) represents the false-positive and false-negative rates as a function of time. The false-positive is the misidentification of normal nodes as bad nodes. The effect of which is normally observed when time is large during which the energy of normal nodes is low, which is likely to reduce the trust value of nodes. However, the false-negative occurs when bad nodes are considered as normal nodes, the effect of it takes place when time is small (initial) at which all nodes in the network are considered to be trustworthy. The graph in figure 10(a) heads towards the discussed outline. The false-negative rate is initially high as all nodes are regarded to be trusted nodes, thus the model is likely to miss the bad nodes. As time progresses, the false-negative rate drop because the proposed solution tends to detect the compromised nodes in the network. But on contrary, the false-positive rate increases slowly since the trust value of normal nodes starts decreasing with time and the system misdiagnoses a normal node as the compromised node. Additionally, the figure illustrates, on average, the model is 95% accurate which increases to 99.99 % at time = 400sec, as false-positive and false-negative rates are lowest at this instant, and then as the time advances the accuracy reduces.

Figure 10(b), shows the sensitivity of the false alarm rate with respect to the trust threshold, below which the node is considered as a compromised node. It can be inferred that as the trust threshold increases, the false-negative rate decreases while the false-positive rate increases. There exists an optimal threshold at which both false-positive and false-negative are minimized. Here for time = 400sec, the optimal trust threshold is 0.5 at which both false-negative and false-positive are zero and the accuracy is maximum, higher than 99.99%.

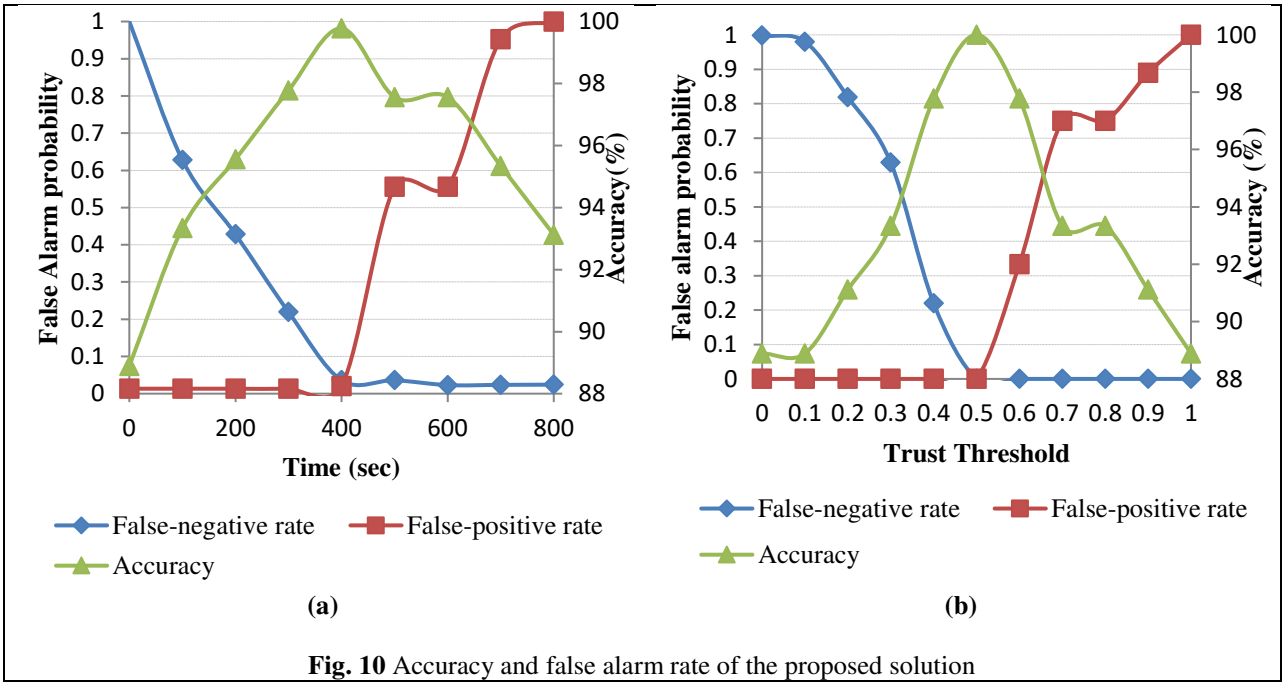


Fig. 10 Accuracy and false alarm rate of the proposed solution

6. Conclusion and future scope

In this paper, we focused on the modeling and analysis of the impact of the node's behavior on network survivability and integrity, which has been rarely studied. Firstly, the node's behavior is classified into four types: adaptive, greedy, mischievous, and crashed state, each with two observable symbols. Then the behavioral model is proposed by employing Hidden Markov Process. The mobile nodes with expected output change their behavior according to the transition probability matrix and emission probability matrix. Once the likelihood of the node being in each behavior state is obtained, the isolation problem is analyzed. The misbehaving nodes whose objective function is to harm the packets are provided with a time-based opportunity (TTR) to reset itself before its permanent isolation. And the selfish nodes whose aim is to drop packets are immediately removed from the network but prior to its removal; nodes are verified to see if they are literally selfish or are at the edge of the crashed state. If nodes drop packets due to minimum residual energy then they are not destroyed but are only removed from the routing function and are given TTL time to regain their lost energy. The scheme adopted helps to increase the survivability of the network. Finally, analytical results were explained by simulation experiments. Besides, our work provides a deeper

understanding of the network performance evaluation in presence of misbehaving nodes like blackhole nodes, greyhole nodes, and sinkhole nodes. Depending upon the application under consideration, it has been realized that for multipoint-to-point traffic; IPV6 Routing Protocol for Low-Power and Lossy network (RPL) is advisable. In that direction, our future work is to include 6LoWPAN and RPL protocols in our proposed HMT models, which can offer customized solution to a wide range of IoT applications. The proposed model considers only two output states as observable states. In future, the behavioral model can further be extended by including more observable symbols like residual resource level and degree of connectivity. The criticality of the model can further be improved by validating it against other attacks like good-mouthing attacks, bad-mouthing attacks, and ballot stuffing attacks.

Declarations

Funding: Not Applicable

Conflicts of interest/Competing interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Availability of data and material: Not Applicable

References

[1] C. K. Dehury and P. K. Sahoo, "Design and implementation of a novel service management framework for IoT devices in cloud," *J. Syst. Softw.*, vol. 119, pp. 149–161, Sep. 2016, doi: 10.1016/j.jss.2016.06.059.

[2] A. K. Akhtar and G. Sahoo, "Mathematical Model for the Detection of Selfish Nodes in MANETs," *Int. J. Comput. Sci. Informatics*, vol. 5, no. 3, pp. 25–28, 2012.

[3] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, K. Saleem, and V. Furtado, "LOADng-IoT: An Enhanced Routing Protocol for Internet of Things Applications over Low Power Networks," *Sensors*, vol. 19, no. 1, p. 150, Jan. 2019, doi: 10.3390/s19010150.

[4] J. Zhongqiu, Y. Shu, and W. Liangmin, "Survivability Evaluation of Cluster-Based Wireless Sensor Network under DoS Attack," in *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*, 2009, doi: 10.1007/978-3-642-32427-7_18.

[5] P. Theerthagiri, "FUCEM: futuristic cooperation evaluation model using Markov process for evaluating node reliability and link stability in mobile ad hoc network," *Wirel. Networks*, vol. 26, no. 6, pp. 4173–4188, Aug. 2020, doi: 10.1007/s11276-020-02326-y.

[6] M. Maragatharajan, C. Balasubramanian, and S. P. Balakannan, "A secured MANET using position-based opportunistic routing and SEMI MARKOV process," *Concurr. Comput. Pract. Exp. , Wiley*, vol. 31, no. 14, pp. 1–8, Jul. 2019, doi: 10.1002/cpe.5047.

[7] L. Chen *et al.*, "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey," *IEEE Access*, vol. 5, no. c, pp. 8956–8977, 2017, doi: 10.1109/ACCESS.2017.2695525.

[8] S. Peng, M. Wu, G. Wang, and S. Yu, "Propagation model of smartphone worms based on semi-Markov process and social relationship graph," *Comput. Secur.*, vol. 44, pp. 92–103, Jul. 2014, doi: 10.1016/j.cose.2014.04.006.

[9] J. Sengathir and R. Manoharan, "A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs," *EURASIP J. Wirel. Commun. Netw.*, vol. 2015, no. 1, p. 158, Dec. 2015, doi: 10.1186/s13638-015-0384-4.

[10] X. Liu and A. Datta, "Modeling context aware dynamic trust using hidden markov model," in *Proceedings of the National Conference on Artificial Intelligence*, 2012, vol. 3, pp. 1938–1944.

[11] P. Pathak, E. Chauhan, S. Rathi, and S. Kosti, "HMM-Based IDS for Attack Detection and Prevention in MANET," in *Lecture Notes in Networks and Systems*, vol. 10, 2018, pp. 413–421.

[12] C.-M. Chen, D.-J. Guan, Y.-Z. Huang, and Y.-H. Ou, "ANOMALY NETWORK INTRUSION DETECTION USING HIDDEN MARKOV MODEL," in *International Journal of Innovative Computing, Information and Control*, 2016, pp. 569–580.

[13] D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in Mobile Social Networks," *Futur. Gener. Comput. Syst.*, vol. 87, pp. 803–815, Oct. 2018, doi: 10.1016/j.future.2017.07.028.

[14] T. Li, Y. Liu, Y. Liu, Y. Xiao, and N. A. Nguyen, "Attack plan recognition using hidden Markov and probabilistic inference," *Comput. Secur.*, vol. 97, p. 101974, Oct. 2020, doi: 10.1016/j.cose.2020.101974.

[15] S. Ingale, M. Paraye, and D. Ambawade, "Enhancing Multi-Step Attack Prediction using Hidden Markov Model and Naive Bayes," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Jul. 2020, no. Icesc, pp. 36–44, doi: 10.1109/ICESC48915.2020.9155895.

[16] A. Roles and H. ElAarag, "Coexistence with malicious and selfish nodes in wireless ad hoc networks: A

Bayesian game approach," *J. Algorithm. Comput. Technol.*, vol. 11, no. 4, pp. 353–365, Dec. 2017, doi: 10.1177/1748301817725305.

[17] J. H. M. Daniel Jurafsky, "Hidden Markov Models," in *Speech and Language Processing (3rd ed. draft)*, vol. 16, no. 9, 2019, pp. 795–796.

[18] B. Todd, A. Ibigbami, and J. Doucette, "Survivable Network Design and Optimization with Network Families," *J. Comput. Networks Commun.*, vol. 2014, pp. 1–12, 2014, doi: 10.1155/2014/940130.

[19] A. H. Azni, R. Ahmad, Z. A. M. Noh, F. Hazwani, and N. Hayaati, "Systematic Review for Network Survivability Analysis in MANETS," *Procedia - Soc. Behav. Sci.*, vol. 195, pp. 1872–1881, Jul. 2015, doi: 10.1016/j.sbspro.2015.06.424.