SIBER-DELTA: **S**warm **I**ntelligence **B**ased **E**fficient **R**outing with **D**istance, **E**nergy, **L**ink quality and **T**rust **A**wareness for Wireless Sensor Networks

V. Neelima and A. R. Naseer

Abstract— Wireless sensor networks are prone to behavior related attacks also termed as insider attacks due to the misbehavior of nodes in forwarding the packets. Trust aware routing is crucial for both securing obtained information as well as protecting the network performance from degradation and network resources from unreasonable consumption due to insider attacks in wireless sensor networks. This paper presents swarm intelligence based Efficient Trust Aware Routing protocol for Wireless Sensor Networks termed as SIBER-DELTA which takes into account trust rating of the nodes along with energy, distance, link quality of the path to select the best quality path from source to sink for packet forwarding. The performance evaluation of our proposed Trust-Aware Routing approach SIBER-DELTA was conducted using NS-2 Simulator considering non-forwarding attacks in both Static and Dynamic Scenarios with varying network sizes. Our simulation results indicate that SIBER-DELTA performs extremely well in terms of malicious nodes detection and avoidance, Packet Delivery Ratio, Energy Efficiency and Latency.

Index Terms— Ant colony based Routing, Forwarder Selection Function, Node Misbehavior, Non Forwarding Attacks Pheromone Update Model, Reputation System, Swarm Intelligence, Trust Aware Routing, Trust Model, Wireless Sensor Networks.

1 INTRODUCTION

WIRELESS sensor networks are gaining immense popularity in industry, military, and academia due to the fact that these networks made of tiny sensor nodes provide low cost solutions to a wide variety of real-world challenges[1]. For most of the mission critical applications, WSNs are to be deployed in harsh and hostile environments unattended where critical security issues need to be considered due to various types of threats and attacks they are exposed to. In addition to having robust key management schemes to secure the network from external attacks [2], WSN requires strategies to mitigate the effect of insider attacks by detecting the misbehavior nodes refusing to participate in packet delivery thereby launching non-forwarding attacks. These behavior related attacks can be thwarted by assigning trust rating to nodes in the network based on the reputation they build over a period of time by being trustworthy in participating in the packet delivery.

There are several insider attacks or behavior level attacks that target the routing operation in WSN [2]. In the black-hole attack, adversary nodes do not forward packets completely, where as in grey-hole attack, malicious nodes selectively forward some packets. Most of the insider attackers are Denial of Service (DOS) attacks [3]. In order to appreciate the concept of Trust aware routing, one needs to consider some aspects that highlight the importance of Trust based routing. Firstly, misbehaving nodes in a wireless sensor network can indulge in misrouting packets to wrong destinations leading to misinformation or can deny totally forwarding packets to their destination leading to loss of information. Mission critical applications such as military, health or commercial applications can be very sensitive to these attacks where WSN nodes have the utmost responsibility to carry and deliver very critical and secret information. Hence, it becomes highly essential to design a Trust aware routing protocol to protect data exchange, secure information delivery and maintain and protect the value of the communicated information.

Secondly, misbehavior of nodes can cause performance degradation to a greater extent. Non-forwarding attacks decrease the system throughput since packets will be retransmitted many times and they are not delivered. Denial of service attacks can increase the packet delay since some nodes acting as forwarders will be busy in responding to the attack and hence forced to delay the processing of other packets. An infected WSN network can be partitioned into different parts that cannot communicate among each other due to non-forwarding attacks.

Thirdly, misbehaving nodes also affect network resources. Denial of Service attacks affect resource availability, whether adversary node is considered as a resource for routing or the availability of data itself is considered. Moreover, these attacks

- *A. R. Naseer is Principal & Professor of Computer Science & Engineering, Jyothishmathi Institute of technology & Science (JITS), Karimnagar, affiliated to JNTU Hyderabad, Telangana State, India, Corresponding author -PH-+919052430745. E-mail: dr_arnaseer@hotmail.com*
- *V. Neelima is Associate Professor at the Department of Computer Science & Engineering, JITS Karimnagar and is currently pursuing PhD degree program at JNTU Hyderabad, Telangana State, India, E-mail: neelima.jits@gmail.com*

force the adversary nodes to consume unnecessary energy on packet reception and processing.

In Trust aware routing, the opinion of a node about the behavior of its next forwarder node is considered in the routing decision. This opinion is quantified and termed as Trust metric which should reflect how much a forwarder is expected to behave to forward a packet when it receives from its previous node in the path from source to sink. The computation of trust metric is by itself a challenge as it requires several operational tasks on observing nodes behavior, exchanging nodes' experience and opinions as well as modelling the acquired observations and exchanged knowledge to reflect nodes trust values. A system that performs these tasks to ultimately generate suitable trust rating for nodes is called a reputation system [4]. A reputation system is a type of cooperative filtering algorithm which attempts to determine ratings for a collection of entities that belong to the same community [5,6]. Every entity rates other entities of interest based on a given collection of opinions that those entities hold about each other. Reputation systems have received considerable attention in different fields such as distributed artificial intelligence, economics, evolutionary biology, e-commerce applications and online auctioning, ad hoc and wireless sensor networking, etc. Most of the concepts in reputation systems depend on social networks analogy. In general, any reputation system in the context of WSN should consist of three main components – Monitoring, Rating and Response. Monitoring component is responsible for observing the activities of the neighbor nodes. Rating component will enable the nodes to rate their neighbor nodes based on the node's own observation, other nodes' observations that are exchanged among themselves, the history of the observed node and certain threshold values. Response component has the responsibility of deciding about different possible reactions it can take, like avoiding bad nodes or even punishing them based on the knowledge built by nodes on others' reputations.

Swarm Intelligence research has been largely carried out to reverse engineer and adapt properly the collective behaviors observed in natural systems such as ant colonies, flocks of birds and schools of fishes to design novel algorithms for distributed optimization and Control [7]. Ant Colony systems have successfully tackled the challenges posed by the nature using their inherent appealing characteristics such as adapting to varying environmental conditions, robust and resilient to the failures caused by internal or external factors, achieving complex behaviors and collaborative operation on the basis of a limited set of rules and effective management of constrained resources with global intelligence which is larger than individual capabilities [8]. Similarities could be drawn with ant colony systems when one considers many of the significant challenges to be addressed in practical realization of wireless sensor networking solutions such as resource constraints, absence of centralized control and infrastructure, complexity and dynamicity of large scale networks, need for survivability and self-configurability, and lastly unattended resolution of potential failures.

In this paper, we present SIBER-DELTA, Swarm Intelligence Based Efficient Routing protocol for WSN with Distance, Energy, Link Quality, and Trust Awareness designed specifically to suit the harsh and hostile environment where the WSN nodes are deployed. Harsh and hostile environments represent WSN deployed in the battlefield, forest, disaster prone and unattended areas where environment conditions keep changing drastically and exposure to various types of threats and attacks keeps increasing. Depending on the environment where they are deployed and the prevailing surrounding environmental and networking conditions, it is noticed that link quality and other related parameters (for example, in heterogeneous WSNs, capabilities of individual nodes are also need to be considered) may vary which are not taken into account when selecting the next forwarder by various ant colony based routing algorithms for WSN reported in the literature. Taking these into account, our approach suggests an improved Forwarder Selection Function to select the best next neighbor to forward the packet to the sink node. It is also observed that the Pheromone Update Model varies from one algorithm to another as the parameters used in the computation of the amount of pheromone concentration to be placed on the path traversed by the backward ant differ. Further, it is found that the amount of pheromone computed to be placed on the path during return journey is not proper to reflect that path as the optimal during the simulation period. Strongest path should have largest amount of pheromone whereas weakest path should have least amount of pheromone or almost zero. Among the competing stronger paths for selection, the variations in pheromone concentration should be such that always strongest path (i.e., optimal) is selected. Keeping these in mind, pheromone update model has been designed considering the parameters the forward ant has collected during its travel from source to the destination, i.e., trust rating of the path, available average Energy, minimum energy of the nodes along the path, Number of hops (i.e., distance indicating shortest path), and link quality of the path to reinforce a path with enough pheromone to select that path as the best path to reach the sink from the source.

The rest of the paper is organized as follows. In Section II, we present some of the previous work related to Trust Aware Secure routing approaches for Wireless Sensor Networks. Section III provides detailed discussion on our proposed approach SIBER-DELTA, Swarm Intelligence Based Efficient Routing protocol for WSN with Distance, Energy, Link Quality, and Trust Awareness. The performance evaluation metrics used in our simulation are presented in Section IV. The simulation setup, Results, Performance of evaluation of our approach and discussion are presented in section V, followed by Concluding remarks.

2 PREVIOUS WORK

In this section, we present some of the related work carried out in the area of Trust-aware routing for wireless sensor networks.

Reputation system based framework for Energy Efficient, Trust-enabled Secure Routing for wireless Sensor Network is proposed in [4,9-13]. This work proposes a customized reputation system - Sensor Node Attached Reputation Evaluator (SNARE) [9,10]. SNARE is a collection of protocols and algorithms that interacts directly with the network layer. The system adopts the geographical routing principle to cope with large network dimensions and relies on a distributed trust management system for the detection of malicious nodes. The system consists of three main components; i.e. monitoring component, rating component and response component. The monitoring component, EMPIRE (Efficient Monitoring Procedure In REputation system) [11,13], observes packet forwarding events. Here a monitoring node will not be in a continuous monitoring mode of operation, rather, it will monitor the neighborhood periodically and probabilistically to save resources. When a misbehaving event is detected, it is counted and stored until an update time and then a report is sent to the rating component. The rating component, CRATER (Cautious Rating for Trust Enabled Routing) [12], evaluates the amount of risk an observed node would provide for routing operation. The risk value is a quantity that represents the previous misbehaving activities that a malicious node (a node that drops packet) obtained. This value is used as an expectation for how much risk would be suffered by selecting that malicious node as a router. It is calculated based on the first hand information and the second hand information. The firsthand information is achieved by the direct observation done by the node of concern. Risk values are updated based on the first hand information every time a new misbehavior report is received from the monitoring component. Moreover, if an observed node shows an idle behavior during a certain period, its risk value is reduced. A monitoring node also updates the risk values of its neighbors by second hand information received periodically from some announcers. In this work, system adopts the defensive response approach wherein depending on the trust relations, a node will try to avoid malicious nodes based on the routing decision made by the proposed routing protocol - Geographic, Energy, Trust Aware Routing protocol (GETAR)[4]. GETAR incorporates the trust information along with distance and energy information (routing decisions are based on a weighted routing cost function which incorporates trust, remaining energy and location attributes) to choose the best next hop for the routing operation thus allowing for better load balancing and network lifetime extension. A simple but strong, independent and representative scale to evaluate reputation systems called *REputaion Systems-Independent Scale for Trust On Routing* (RESISTOR) is also proposed in [13].

In [14] Reputation based Framework for High Integrity Sensor Networks (RFSN) is proposed where nodes maintain reputation for other nodes and use it to evaluate their trustworthiness. It provides a scalable, diverse and a generalized approach to tackle misbehaviors resulting from malicious and faulty nodes. It employs a Bayesian formulation using a beta distribution model [15] for reputation representation. Distributed Reputation-based Beacon Trust System (DRBTS) proposed in [16] for excluding malicious beacon nodes providing false location information is aimed at providing a method by which beacon nodes can monitor each other and exchange information so that sensor nodes can choose who to trust, based on a quorum voting approach where a sensor must get votes for its trustworthiness from at least half of their common neighbors. Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks (TIBFIT) to diagnose and mask arbitrary node failures in an event-driven wireless sensor network is proposed in [17]. The goal of the proposed TIBFIT protocol involves event detection and location determination in the presence of faulty sensor nodes, coupled with diagnosis and isolation of faulty or malicious nodes. Parameterized and Localized trUst management Scheme (PLUS) for WSN proposed in [18] adopts a localized distributed approach where trust is calculated based on either direct observations or indirect observations. In [19], Locally Aware Reputation System (LARS) is proposed to mitigate misbehavior and enforce cooperation. Each node only keeps the reputation values of all its one-hop neighbors. The reputation values are updated on the basis of direct observations of the node's neighbors. The misbehaving node is not excluded from the network for ever and it is given a chance to build its reputation by good cooperation over a time-out period to be accepted for routing. A Trust-Aware Routing Framework (TARF) for Wireless Sensor Networks is proposed in [20] to secure multi-hop routing in WSN against intruders exploiting the replay of routing information. This approach identifies the malicious nodes that misuse "stolen" identities to misdirect packets by their low trustworthiness thereby helping the nodes to circumvent adversary nodes which misroute considerable traffic with forged identity attained through replaying. A resilient trust model, SensorTrust with a focus on data integrity for hierarchical WSN proposed in [21] uses the aggregator to maintain trust estimations for children nodes by integrating their long-term reputation and short-term risk and taking into consideration both communication robustness and data integrity. This model employs the Gaussian model to rate data integrity in a fine-grained style, and a flexible update protocol to adapt to different applications.

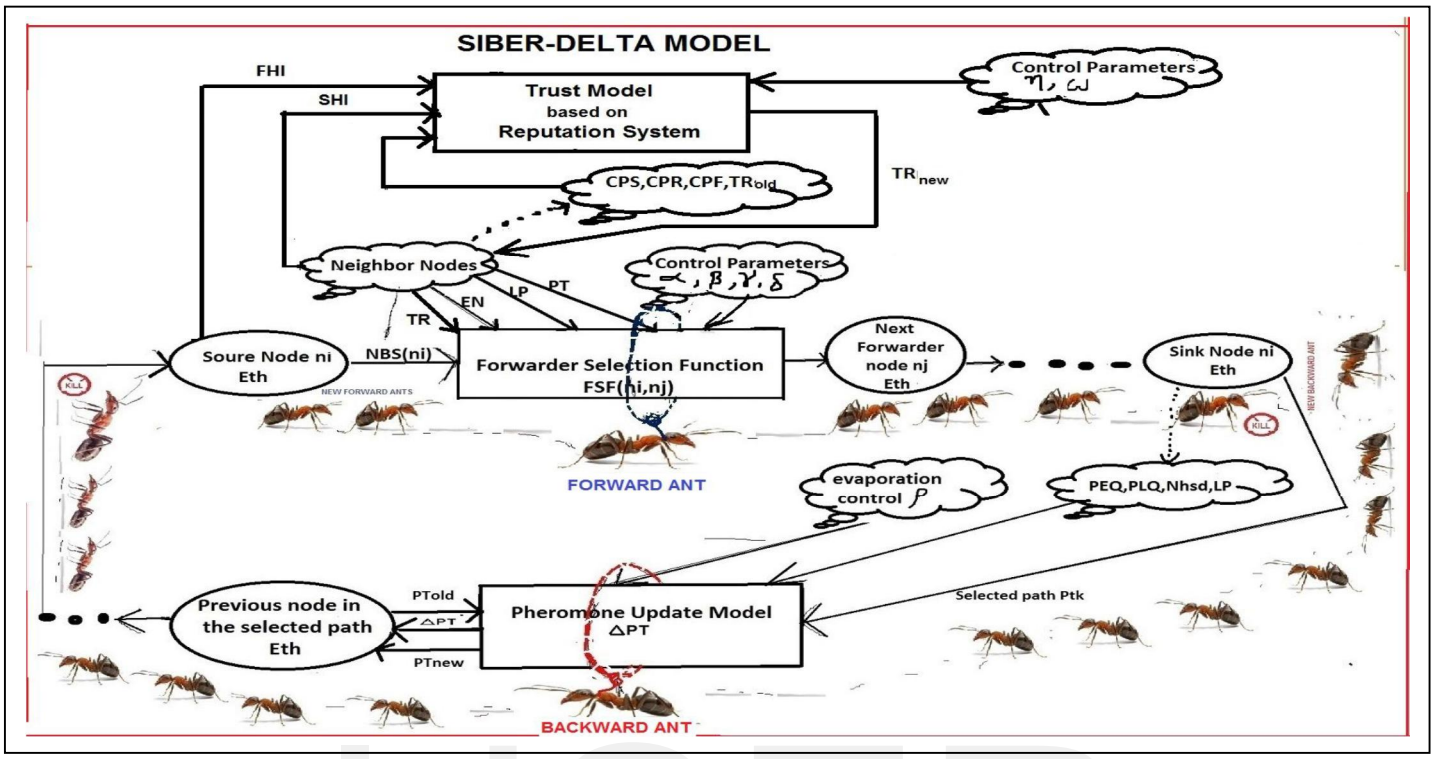


Fig 1. SIBER-DELTA Model

3 Proposed Approach – Siber-Delta

In this section, we present our proposed model SIBER-DELTA, Swarm Intelligence Based Efficient Routing protocol for WSN with Distance, Energy, Link quality and Trust Awareness. This is an extension to our model SIBER-VLP [22] which does not take into account Trust Awareness. Our proposed model SIBER-DELTA is shown in figure 1 which consists of three main components - Trust Model, Optimal Forwarder Selection Function and Improved Pheromone Update Model which are discussed next.

3.1 Trust Model

In our proposed Trust Model, nodes rate each other by using the information of their own direct interactions with their neighbors. This is termed in the literature as First Hand Information(FHI). In order to make the rating unbiased, the nodes also collect their neighbors' interactions with that node being rated considered as Indirect interaction. This rating information collected from the neighbors is also known as Second Hand Information(SHI). The simulation period is now divided into 'n' slots where each slot consists of two sub-periods - Forwarding and Monitoring Interval, T_{FMI} followed by UPdate Interval T_{UPI} as shown in figure 2.

The Forwarding and Monitoring Interval T_{FMI} is the period during which the nodes forward their packets, record the transmission and reception of packets to and from their neighbors. The UPdate Interval, T_{UPI} is the period during which each node computes the Forwarding Misbehavior Index of their neighbors based on First Hand Information and Second Hand Information about their neighbors monitored during the T_{FMI} period. Forwarding Misbehavior Index of the neighbor nodes are used then to determine the Mistrust Index of their neighbors. Finally, Trust ratings of all neighbor nodes participating in packet forwarding are computed.

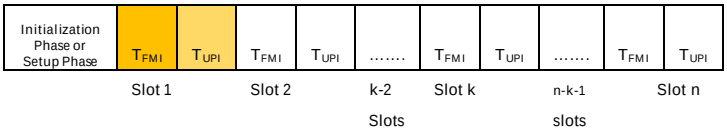


Fig 2. Simulation Period Slots

In our work we consider cooperative monitoring environment, wherein a node does not need to continuously monitor its neighbors' activities as long as there are sufficient set of nodes that can monitor the same activities. So, if an activity can be monitored by two or more nodes who can share their knowledge among each other, then it is enough to have only one monitor active at a time. Then, upon using suitable MAC scheduling approach, the active node sleeps and another one gets awake. We assume that the network has bidirectional links. This means that if node A can send a packet to node B, then node B is also able to send a packet to

node A. This assumption is necessary to guarantee packets overhearing during node's active period. This is because if the link between A and B is bidirectional, then when node A transmits its packet to B, A can hear if B forwards its packet. Otherwise, A will always fail to hear node B if the link is unidirectional from A to B. In this work, we consider only non-forwarding attacks. Other denial of service attacks are considered as future work.

Based on its own evaluation of its neighbors, each node computes Forwarding Misbehavior Index of each neighbor node based on First Hand Information.

Let CPS(ni, nj) be the count of the packets sent by node ni to forwarding node nj. Let CPR(nj, ni) be the count of the packets received by forwarder node nj from current node ni. Let CPF(nj,ni,nk) be the count of the packets pertaining to node ni forwarded by node nj to next forwarder nk.

The Forwarding Misbehavior Index of a neighbor forwarder node nj evaluated by current node ni based on First Hand Information or Direct Interactions, DIFMI is given by

$$DIFMI(ni, nj) = \frac{CPR(ni,nj) - CPF(nj,ni,nk)}{CPS(ni,nj)} \quad -(1)$$

Based on the evaluation information received from its neighbors, each node computes the Forwarding Misbehavior Index of each neighbor node based on Second Hand Information received from their neighbors.
The Forwarding Misbehavior Index of a neighbor forwarder node nj evaluated by current node ni based on Second Hand Information or InDirect Interactions, IDFMI is given by

$$IDFMI(ni,nj) = \frac{\sum_{nk \in NBS(ni)} FMI(nk,nj) * TR(nk)}{|NBS(ni)| - 1} \quad -(2)$$

Where nk ≠ ni, nj and NBS(ni) is the neighbor node set of node ni.
Now, the Mistrust Index, MI of neighbor node nj as computed by current node ni can be given by

$$MI(nj,ni) = \eta * DIFMI(ni,nj) + (1-\eta) * IDFMI(ni,nj) \quad -(3)$$
$$\text{where } 0 < \eta \leq 1$$

Higher value of η indicates higher importance given to First Hand Information. η can be used to decrease the importance of DIFMI if the trust rating of current node ni is lower than the trust rating associated with its neighbors so that IDFMI can prevail over DIFMI or both can be given equal importance depending on the requirements by making $\eta = 0.5$.
Now the Current Trust Rating of nj as assigned by node ni can be given by

$$TR(nj,ni)^{curr} = 1 - MI(nj,ni) \quad -(4)$$

As Mistrust Index gets lower value, trust rating attached to the node increases. When Mistrust Index MI(nj,ni) =0, then the trust rating of nj, $TR(nj,ni)^{curr} = 1$ which indicates that node nj is the most trustworthy forwarder node as far as ni is concerned and also recommended by its neighbors. When Mistrust Index MI(ni, nj) = 1, then the trust rating of nj, $TR(nj,ni)^{curr} = 0$, which indicates that node nj is the most untrustworthy node among the neighbors. Hence, it cannot be used as a forwarder node and should be avoided in the forwarding path as a punishment for showing severe misbehavior of dropping all the packets which represents the case of non-forwarding attack, Black Hole.

Now to provide some incentives to the node which has participated very actively in forwarding packets earlier, i.e., for showing very good behavior in the past, the Trust Rating of the nodes can be augmented by considering the previous Trust rating of that node, i.e., Trust Rating of that node in the previous UPdate Interval, T_{UPI}, call it $TR(nj,ni)^{old}$ (i.e., $TR(nj,ni)^{old} = TR(nj,ni)^{curr}$ of previous update period, T_{UPI}) and incorporating it in the equation with some weightage.

Hence, new Trust Rating of node nj as seen by node ni can be rewritten as

$$TR(nj,ni) = \omega * TR(nj,ni)^{curr} + (1-\omega) * TR(nj,ni)^{old} \quad -(5)$$
$$\text{where } 0 < \omega \leq 1$$

The weightage factor ω can be varied to give some incentives to the nodes for their good past behavior by incorporating some suitable amount of past trust value. This can even be more generalized by considering the performance of that node over past m time slots of the simulation i.e., considering the past history of the node in sincerely forwarding packets instead of considering its behavior in one previous time slot.

Assuming that we are currently in the kth timeslot of the simulation period where k > m,

Then the past history of the node nj over the past m time slots is given by the average of its Trust Rating over the last m time slots

$$TR^{m}_{avg}(nj) = \frac{\sum_{ph=k-m}^{k-1} TR(nj,ph)}{m} \quad -(6)$$
$$\text{where ph indicates the time slot}$$

Hence, new Trust rating of node nj as seen by node ni can be rewritten as

$TR(nj,ni) = \omega * TR(nj,ni)^{curr} + (1-\omega) * TR^{m}_{avg}(nj)$ -(7)
where $0 < \omega \leq 1$

This will also handle selective forwarding attacks. Selective forwarding nodes can be given some chance to remain in the network by improving their trust value considering their past good behavior instead of punishing them out-rightly by avoiding them completely in the forwarding path throughout the simulation as done for Black Holes.

3.2 Forwarder Selection Function

To select the best next neighbor to forward the packet to the sink node, a Forwarder Selection Function is used at every node along the path from source to sink node in the network. The Forwarder Selection Function is a probability function which must always choose an optimal path from source to the sink to forward the packets with multiple objectives:

(i) to provide a secure trustworthy path from source to sink by avoiding insider attacks,
(ii) to improve the Network Lifetime by balancing the energy among the nodes in the network to ensure that some nodes along the path do not get depleted fast (resulting in Network disconnections or partitioning)
(iii) at the same time selecting good quality links along the path to guarantee that node energy is not wasted due to too frequent retransmissions.
(iv) Further, selection of shorter paths involving less number of nodes resulting in further saving of energy due to less number of nodes participating in packet forwarding.

Forwarder Selection Function, FSF, is proposed considering the above multiple objectives to select the best forwarder node among the neighboring nodes of the current node, which is based on Pheromone Trail(PT) and heuristic function involving three parts representing Node Trust Rating (TR), Node Energy Level(EN) and Node Link Quality(LP) functions. Pheromone Trail(PT) represents the concentration of pheromone deposited on the path between the nodes (i.e., current node and its neighbor node) considering trust, energy, distance and link quality along the path (containing the link between current and neighboring nodes) from source to destination. In other words, higher PT represents the better good quality trustworthy path from source node to the destination in terms of trust, energy, distance and link quality. Node Trust Rating (TR) represents the trust rating assigned to the neighbor node, Node Energy (EN) function represents energy level of the neighbor node and Link quality(LP) function represents the quality of the link between the current node and the neighbor node under consideration.

Hence, the Forwarder Selection Function, FSF(ni, nj) to select the best forwarder node nj among the neighboring nodes of the current node ni can be defined as

$$FSF(ni,nj)= \begin{cases} \frac{[PT(ni,nj)]^{\alpha}[EN(nj)]^{\beta}[LP(ni,nj)]^{\gamma}[TR(ni,nj)]^{\delta}}{\sum_{nj \in NBS(ni)}[PT(ni,nj)]^{\alpha}[EN(nj)]^{\beta}[LP(ni,nj)]^{\gamma}[TR(ni,nj)]^{\delta}}, & if\ nj \in NBS(ni), \\ 0, & otherwise \end{cases}$$ -(8)

where NBS(ni) represents the set of neighboring nodes of ni, PT(ni,nj) represents the concentration of pheromone deposited on the path between the nodes ni and nj, EN(nj) represents the energy level of the neighbor node nj. TR(ni, nj) represents the Trust rating of the neighbor node nj as given by node ni.

LP(ni,nj) represents the quality of the link between nodes ni and nj, i.e., link probability. The Expected Transmission Count, ETX is a measurement of the transmission link which is calculated based on the past events occurred on that link.
Then the link probability LP(ni, nj) between nodes ni and nj is given by the expression :

$$LP(ni, nj) = \frac{1}{ETX(ni,nj)}$$ -(9)

$\alpha, \beta, \gamma, \delta$ are the parameters to control the significance or importance of pheromone trail of the path, node energy level, link quality between nodes and node trust rating. When $\alpha = \beta = \gamma = \delta = 1$, all four parameters PT, EN, LP, TR are given equal importance in the selection of the forwarder node. If one is interested in giving higher importance to TR, node trust rating, then one could make $\alpha = \beta = \gamma = 2, \delta = 1$, similarly $\alpha = 2, \beta = 1, \gamma = \delta = 2$ to raise importance of EN, Node Energy Level, $\alpha = 2, \beta = \delta = 2, \gamma = 1$ to make importance of link quality more significant in the selection of forwarder node.

Let EI(nj) be the initial energy of node nj and ER(nj) be the Remaining (Actual) Energy of node nj, then the Node Energy level, EN(nj) is defined as

$$EN(nj) = \frac{ER(nj)}{EI(nj)} \text{ where } ER(nj) > Eth$$ -(10)

Threshold Energy, Eth is defined as the energy at which the node loses its right to participate in packet forwarding and is excluded from the path. Actual Energy of the neighboring node should be greater than the threshold Energy Eth in order to be considered for selection.

Moreover, Eth can be used as a tunable parameter which can be varied depending on the traffic or load. For example, to conserve energy for later use and to perform load balancing, initially Eth can be raised to 50% of the Initial Energy EI so that most of the nodes will participate in packet

forwarding/processing till the threshold energy is reached rather than some nodes getting depleted faster due to the prevailing higher importance attached to other two parameters. Later depending on the traffic or type of processing, Eth can be lowered to a reasonable value in order to extend the lifetime of the network [23].

3.3 Pheromone Update Model

It has been observed that the amount of pheromone computed to be placed on the path during return journey is not proper to reflect that path as the optimal during the simulation period. Strongest path should have largest amount of pheromone whereas weakest path should have least amount of pheromone or almost zero. Among the competing stronger paths for selection, the variations in pheromone concentration should be such that always strongest path (i.e., optimal) is selected.

Keeping these in mind, pheromone update model has been designed considering the parameters the forward ant has collected during its travel from source to the destination. Once the forward ant reaches the destination, the following parameters collected by the forward ant are analyzed.

- Eavg, Average Energy of the nodes in the path traversed by forward ant
- Emin, Minimum Energy of the nodes in the path traversed by forward ant
- Nhsd, Distance travelled by the forward ant from source to destination, i.e., number of hops
- Ptk, Path traversed by forward ant k from source to destination having Nhsd(Ptk) hops
- LP(Ptk), Average Link probability of the path traversed by the forward ant from source to sink
- NS(Ptk), Set of nodes along the path Ptk travelled by the forward ant from source to destination
- PTR(Ptk), Trust Rating of the path Ptk

Average ETX of the links in the path Ptk,

$$ETX_{av}(Ptk) = \frac{\sum_{i=1}^{Nhsd(Ptk)} ETXi}{Nhsd(Ptk)} \quad -(11)$$

Average Link Probabilities of path Ptk,

$$LP(Ptk) = \frac{1}{ETXav(Ptk)} \quad -(12)$$

Hence Link Quality of the Path (Ptk) is given by

$$\text{Path Link Quality, } PLQ(Ptk) = \frac{1}{ETXav(Ptk)*Nhsd(Ptk)}$$

$$= \frac{\text{LP(Ptk)}}{Nhsd(Ptk)} \quad -(13)$$

The Path Energy Quality is represented by the Average Energy, Eav, and Minimum Energy, Emin of the nodes along the path. Hence, Energy Quality of Path, Ptk is given by the following expression:

Path Energy Quality,

$$PEQ(Ptk) = \frac{E_{avg}}{E_{in}} - \left(1 - \frac{E_{min}}{E_{avg}}\right) \quad -(14)$$

Higher Average Energy and higher Minimum Energy of nodes along the path would yield a good quality path in terms of Energy.

Trust Rating of path Ptk is given by the following expression :

$$\text{Path Trust Rating, } PTR(Ptk) = \frac{\sum_{nk \in NS(Ptk)} TR(nk)}{|NS(Ptk)|} \quad -(15)$$

The Pheromone update or the concentration of additional pheromone to be deposited is computed as given by the following expression:

ΔPT = Path Energy Quality * Path Link Quality * Path Trust Rating -(16)

= PEQ(Ptk) * PLQ(Ptk) * PTR(Ptk)

$$= \left(\frac{E_{avg}}{E_{in}}\left(1 - \frac{E_{min}}{E_{avg}}\right)\right) * \frac{\text{LP(Ptk)}}{Nhsd(Ptk)} * \frac{\sum_{nk \in NS(Ptk)} TR(nk)}{|NS(Ptk)|} \quad -(17)$$

The equation (17) captures the impact of Average Energy and Minimum Energy of the nodes along the trustworthy path with better path link quality on the concentration of pheromone deposition. In other words, good quality higher trust rating path with high average energy and higher value of minimum energy will result in more amount of pheromone to be deposited on that path rather than the path with low trust rating, minimum and average energy.

Once the forward ant reaches the destination, ΔPT is computed using the parameter values provided by the forward ant and the forward ant is killed.

Next backward ant is created at the sink node with the computed ΔPT and Nhsd. The Pheromone updating is done by the backward ant in the reverse direction during its travel from destination node to source node.

For situations where nodes nearer to the destination node to have higher pheromone deposition when compared to nodes nearer to the source node in the path, the ΔPT computed in (16) is updated by the backward ant in the following fashion.

$$\Delta PT = \Delta PT_{*} \left(1 - \frac{Nhcd-1}{\text{Nhsd}}\right) \quad \text{-(18)}$$

where Nhcd is the number of hops from current node to the destination node during the traversal of the backward ant from destination to the source node.

Whenever a node ni receives a backward ant coming from a neighboring node nj, it updates $PT(ni, nj)$ in its routing table in the following manner:

$$PT(ni, nj) = (1 - \rho)PT(ni, nj) + \Delta PT \quad \text{-(19)}$$

where ρ is a decay coefficient and (1- ρ) represents the evaporation of Pheromone Trail since the last time of updating of $PT(ni, nj)$.

5 Simulation Setup, Results & Discussion

Our proposed system, SIBER-DELTA was simulated using open source NS-2 simulator. In this simulation, we have considered static and dynamic network scenarios with random topology with nodes randomly distributed. Random way-point mobility model is used for dynamic network with the nodes having the ability to move with a specified speed. Our proposed trust enabled routing approach SIBER-DELTA is compared with SIBER-VLP [22] without trust awareness for varying network sizes(dimension) – 50 and 100 nodes by introducing 10%, 20% and 30% non-forwarding attackers in the network. It is assumed that all the methods use the same data rate. The performance evaluation metrics used in this simulation are Packet Delivery Ratio, Latency, Dropped packets, Average Energy Consumed, Average Energy Remaining, Minimum Energy, Energy Efficiency(Kb/J), and Standard Deviation which are presented in section 5.1

5.1 Performance Evaluation Metrics

In this section, we present the Performance Metrics used in the evaluation of our proposed Approach: SIBER-DELTA.

(i) Packet Delivery Ratio is defined as

$$\text{PDR} = \frac{\text{Total number of packets delivered at the sink node}}{\text{Total number of packets generated at the source node}} \quad \text{-(20)}$$

(ii)Energy Efficiency is defined as

$$\text{EE} = \frac{\text{Total number of packets delivered at the destination}}{\text{Total energy consumed by the sensor nodes in the network}} \quad \text{–(21)}$$

(iii)Total Energy Consumed is defined as the total energy consumed (in joules) by the nodes in the network during the period of simulation.

(iv)Latency is defined as the difference in time when a packet is generated at the source node and when it eventually gets delivered at the sink node, that is nothing but the time delay of a packet sent from the source node to reach the destination node.

(v) Standard Deviation σ is defined as the average variation between energy levels of all nodes in the network (in joules)

$$\sigma = \sqrt{\frac{\sum_{i=0}^{NS-1}(ERni - \mu)^2}{NS}} \quad \text{-(22)}$$

where NS is the total number of nodes in the network, ERni is the remaining energy of node ni in the network and μ is the mean of the energy levels of all the nodes in the network.

5.2 Simulation Setup – Static Scenario

The simulation parameters used in the simulation study are shown in Table 1.

Table 1 : Static Scenario - Simulation Parameters

Parameter	Value
Scenario	Static
Topology	Random
Number of Nodes	50, 100
Area	600 X600, 900X900
Transmission Radius	250 meters
Propagation Model	TwoRayGround
Initial Energy	30J
Transmitting Energy	1.0mW
Receiving Energy	0.5mW
Packet Size	1000 bytes
Bandwidth	11MB
Simulation Time	100 sec
Data Traffic	CBR
Data Rate	50Kbps
α	2
β	2
γ	1
δ	1
ϱ	0.2

5.3 Results and Discussion - Static Scenario

In static scenario, all nodes including the destination node are fixed. Our proposed trust aware routing approach SIBER - DELTA is compared with SIBER-VLP [22] without trust awareness for varying network sizes – 50 and 100 nodes by introducing 10%, 20% and 30% attackers and the results for each network size are presented in the following sections.

5.3.1 Static Scenario – Network Size = 50 Nodes with 10%, 20% and 30% Non-Forwarding attackers

The simulation results for 50-node static network with 10%, 20% and 30% malicious nodes are presented in this section.

(i) Without Trust Awareness

In this simulation, first we used our developed protocol SIBER-VLP [22] without trust awareness to determine the impact of introducing 10%, 20% and 30% non-forwarding attackers on the performance of the network. As it is seen from fig. 3a) SIBER-VLP model exhibits performance degradation as malicious nodes are introduced in the network. Fig. 3b) clearly shows that as the number of malicious nodes increases, we observe an increase in packet drops due to the presence of more malicious nodes in the paths selected by the ants. SIBER-VLP with 10% malicious nodes shows on an average a success rate of 75.34%, with the presence of 20% malicious nodes shows a success rate of 30.63% and with 30% of the nodes as malicious shows very poor performance with an average success rate of 20.27%.

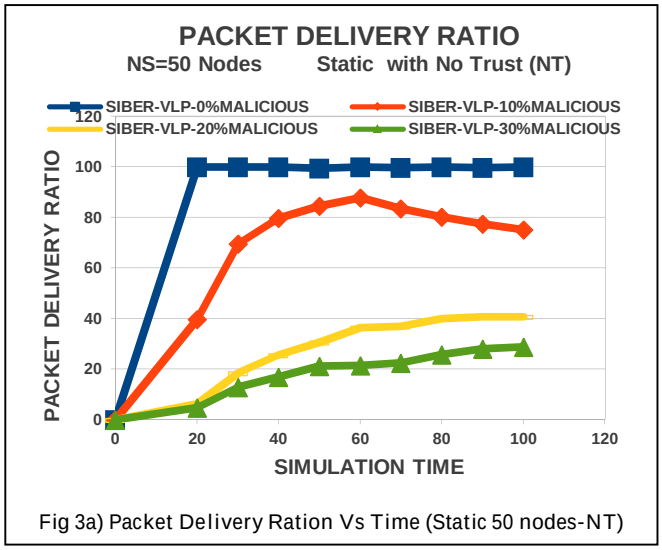


Fig 3a) Packet Delivery Ration Vs Time (Static 50 nodes-NT)

As far as Energy efficiency is concerned (fig 3c)), Energy Efficiency of SIBER-VLP with malicious nodes decreases based on the number of malicious nodes or attackers in the network.

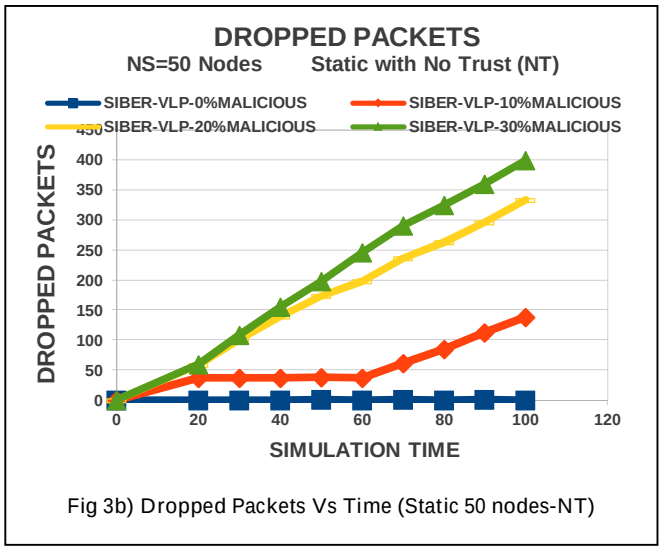


Fig 3b) Dropped Packets Vs Time (Static 50 nodes-NT)

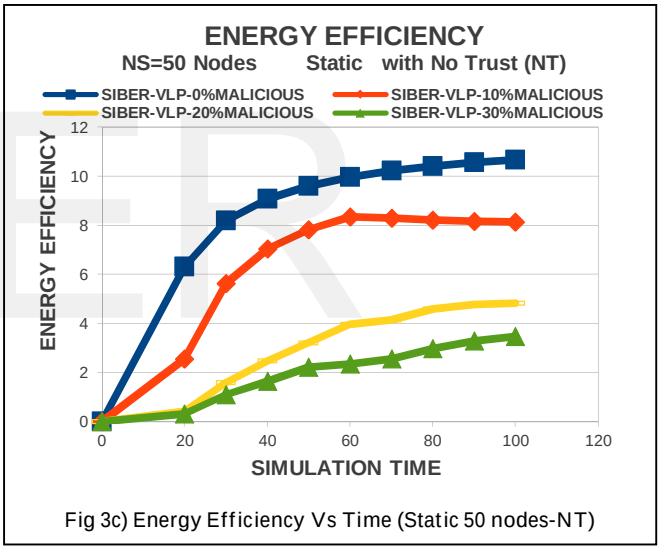


Fig 3c) Energy Efficiency Vs Time (Static 50 nodes-NT)

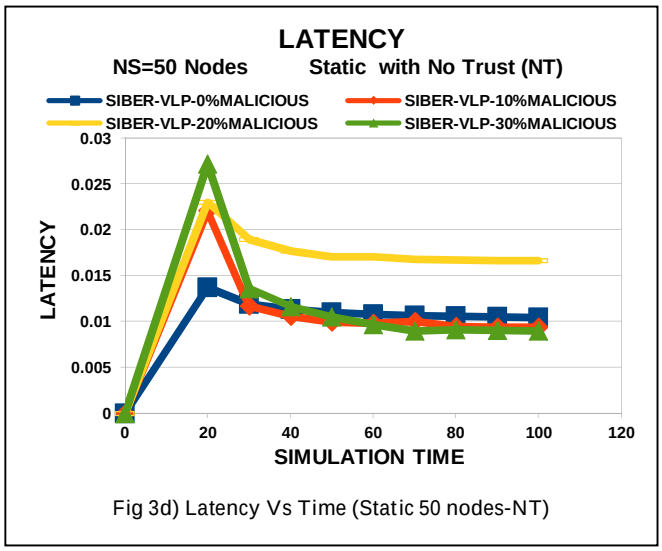


Fig 3d) Latency Vs Time (Static 50 nodes-NT)

When compared to SIBER-VLP without malicious nodes, Energy Efficiency decreases sharply with 20.44% decrease for 10% attackers, 48.68% decrease for 20% attackers and followed by a high reduction of 63.28% for 30% attackers as large number of packets are not delivered to the destination due to the presence of more attackers along the path to the sink.

As evident from figure 3d), SIBER-VLP with no malicious nodes uses high quality paths having less number of hops, thereby reducing the end to end delay. It is clearly seen that latency increases initially with the introduction of attackers as it takes more time to send packets to the sink at the start of the simulation due to large network size. But later as the packet drops increase due to the presence of malicious nodes in selected paths, it transmits less number of packets to the sink but selecting better quality alternate paths with less number of hops to attain energy balancing, in effect decreasing the latency.

As shown in figs. 3e), with the introduction of more & more attackers, due to the presence of less number of paths to the sink and energy balancing among the nodes along the existing paths, the energy consumption is not that high when compared to SIBER-VLP with no malicious nodes.

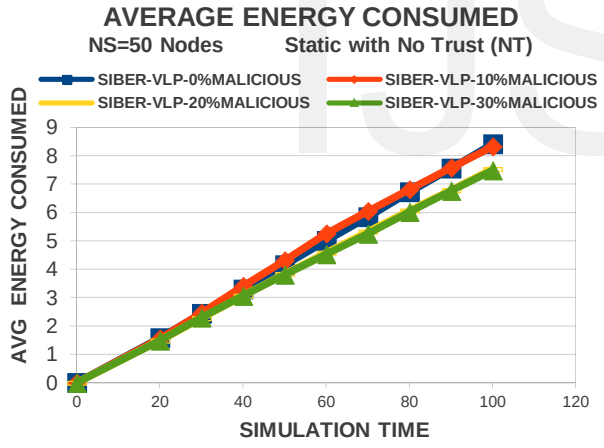


Fig 3e) Avg Energy Consumed Vs Time (Static 50 nodes-NT)

It is to be noted that SIBER-VLP with no malicious nodes should consume little higher energy (which is also seen in fig 3e)) as it achieves higher packet delivery ratio with more number of nodes along good quality paths participating in packet forwarding without any hindrance. Moreover, remaining energy and minimum available energy will also be at a slightly higher value due to less delivery of packets to the destination as evident from fig 3f) and 3g) with lower standard deviation (fig 3h)).

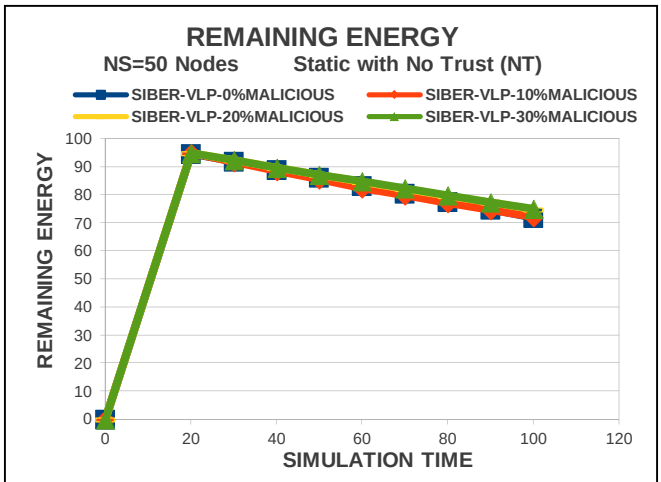


Fig 3f) Remaining Energy Vs Time (Static 50 nodes-NT)

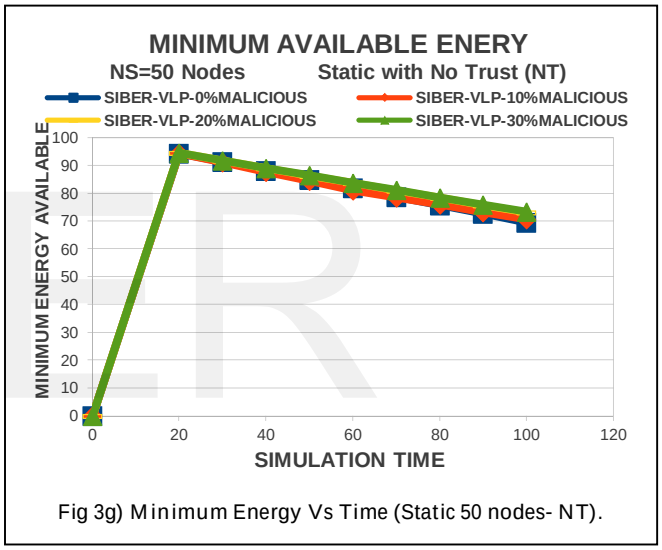


Fig 3g) Minimum Energy Vs Time (Static 50 nodes- NT).

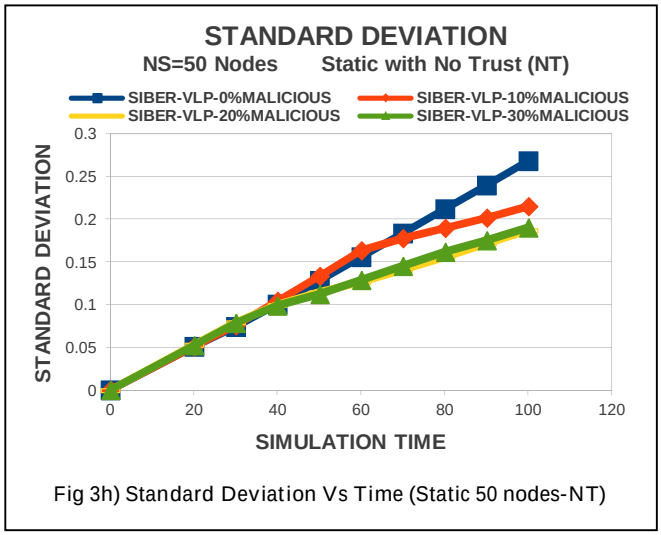


Fig 3h) Standard Deviation Vs Time (Static 50 nodes-NT)

(ii) With Trust Awareness

Next we study the performance of our proposed trust aware routing protocol SIBER-DELTA in the presence of 10%, 20% and 30% attackers for static network size of 50 nodes.

In our model, all nodes are assigned initially equal trust rating during the initialization and setup phase. Hence, there will be some packet drops initially immediately after the initialization and setup phase as nodes encounter neighbour nodes with equal trust rating. During the first slot of the simulation period, behaviour of nodes are evaluated in Forwarding and Monitoring Interval, T_{FMI} and new trust ratings are assigned to the nodes during the UPdate Interval T_{UPI}. This process of new node rating computation and updating is continued in all the time slots of the simulation period.

It is clearly seen from fig. 4a) that SIBER-DELTA model with trust implementation exhibits high packet delivery ratio. By avoiding completely untrusted nodes and considering only trusted nodes (i.e., nodes with higher trust rating) along the paths from source to sink, SIBER-DELTA is able to achieve a high success rate of 99.51% with 10% attackers, 98.88% with 20% attackers and 98.35% with 30% attackers in the network. Since very less number of packet drops are observed during the entire simulation, it can be concluded that SIBER-DELTA performs extremely well by detecting all malicious nodes along the paths from source to sink and preventing these untrusted nodes from packet forwarding completely to achieve higher observed success rate.

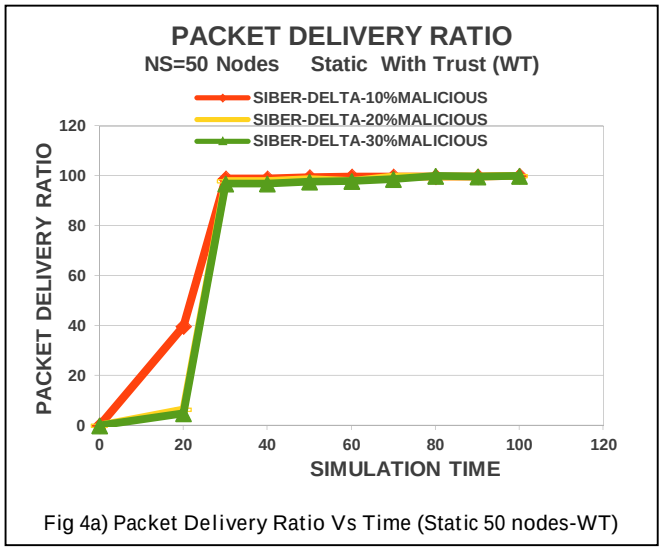


Fig 4a) Packet Delivery Ratio Vs Time (Static 50 nodes-WT)

Further, end to end delay or latency has been low and almost uniform due to the quality paths selected among the existing paths as shown in fig 4b) in the case of SIBER-DELTA with 10% and 20% malicious nodes. Whereas latency is slighter higher in the case of 30% attackers as it has to take longer alternate paths (i.e., paths with higher hop count) in order to avoid black holes existing in the shorter paths.

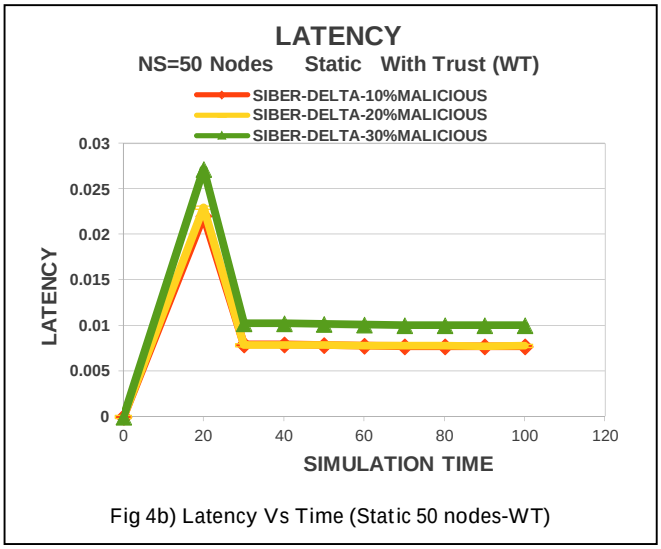


Fig 4b) Latency Vs Time (Static 50 nodes-WT)

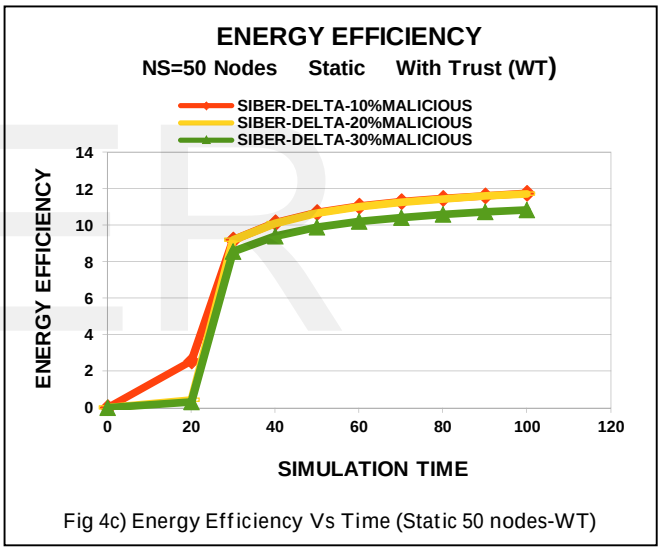
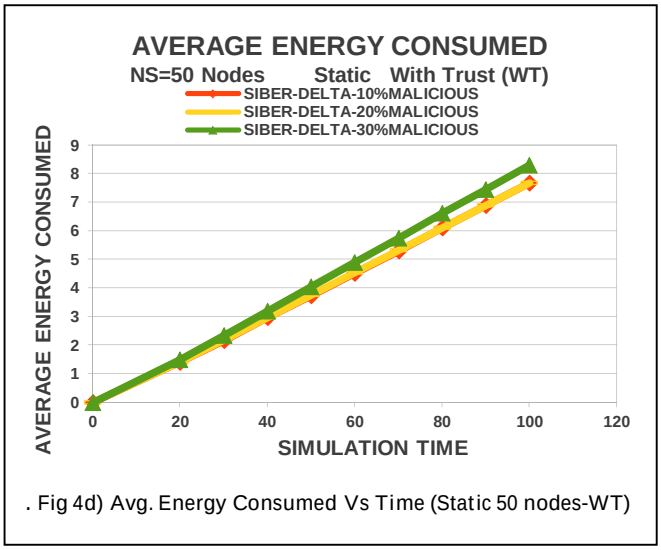


Fig 4c) Energy Efficiency Vs Time (Static 50 nodes-WT)



. Fig 4d) Avg. Energy Consumed Vs Time (Static 50 nodes-WT)

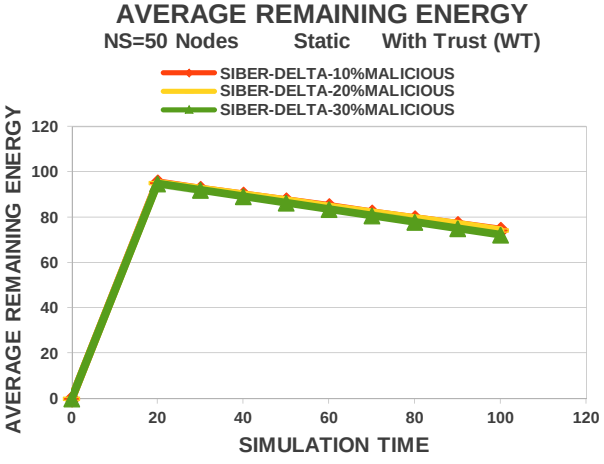


Fig 4e) Remaining Energy Vs Time (Static 50 nodes-WT)

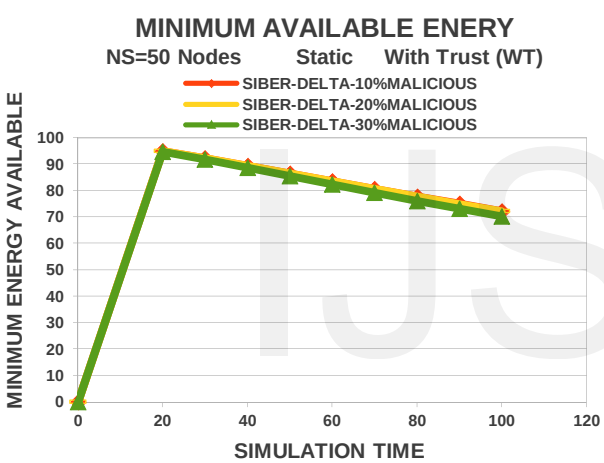


Fig 4f) Minimum Energy Vs Time (Static 50 nodes- WT).

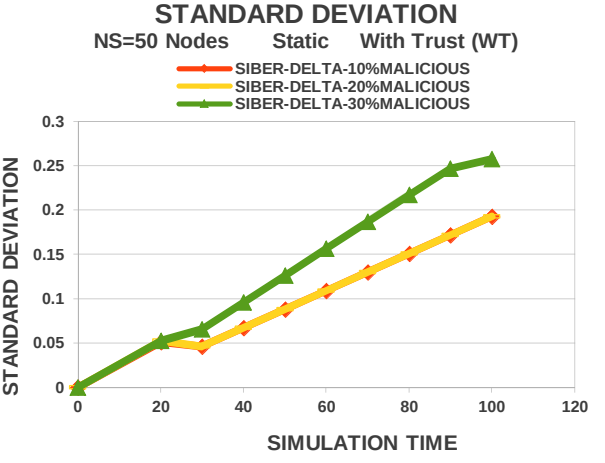


Fig 4g) Standard Deviation Vs Time (Static 50 nodes-WT)

As evident from Fig. 4c), SIBER-DELTA shows higher Energy Efficiency in the case of 10% and 20% attackers and slightly lower Energy Efficiency for 30% attackers as it consumes slightly higher energy due to the selection of longer alternate paths with more nodes to avoid black holes. Moreover, energy consumption has been moderate as seen in fig 4d). The Remaining Energy (fig 4e)), Minimum Energy available (fig 4f)) and Standard Deviation (fig 4g)) plots clearly indicate the energy balancing among the nodes participating in packet forwarding or delivery in the network.

5.3.2 Static Scenario – Network Size = 100 Nodes with 10%, 20% and 30% Non-Forwarding attackers

In this section, we present the simulation results for 100-node static network with 10%, 20% and 30% malicious nodes.

(i) Without Trust Awareness

First, we simulate our protocol SIBER-VLP without trust awareness to study the effect on the network performance in the presence of 10%, 20% and 30% non-forwarding attackers in the network. As malicious nodes are introduced in the network, the performance of SIBER-VLP degrades as shown in fig 5a). It is clearly seen from figure 5 b) that the packet drops increase enormously with the increased presence of malicious nodes in the paths selected by the ants to the sink. As evident from fig 5a), SIBER-VLP with 10% attackers shows a decreased average success rate of 50.16%, with 20% attackers the packet delivery ratio reduces to 33.68% and with 30% attackers, it further reduces to 24.97%. Overall success rate degrades with the percentage increase of malicious nodes in the network when compared to network without non-forwarding attackers.

It is clearly seen from fig 5c) that latency increases initially with the introduction of attackers as it takes more time to send packets to the sink at the start of the simulation due to large network size. But later as the packet drops increase due to the presence of malicious nodes in selected paths, it transmits less number of packets to the sink but selecting better quality alternate paths with less number of hops to attain energy balancing, in effect decreasing the latency. SIBER-VLP with no malicious nodes shows reduced end to end delay as it uses high quality paths having less number of hops.

It is observed in fig 5d) that the Energy Efficiency of SIBER-VLP with malicious nodes decreases as percentage of attackers increase in the network. With the introduction of more and more attackers, the Energy Efficiency drastically decreases to 50% to that observed for SIBER-VLP without

malicious nodes. This is because large number of packets are not delivered to the sink due to the presence of more attackers along the paths to the sink.

Due to the presence of less number of paths to the sink and energy balancing among the nodes along the existing paths, the energy consumption is not that high in the case of SIBER-VLP with malicious nodes as shown in figs. 5e). It is to be noted that SIBER VLP with no malicious nodes consumes little higher energy as it achieves higher packet delivery ratio with more number of nodes along good quality paths participating in packet forwarding without any hindrance. Moreover, remaining energy and minimum available energy will also be at a slightly higher value due to less delivery of packets to the destination as evident from fig 5f) and 5g) with lower standard deviation (fig 5h)).

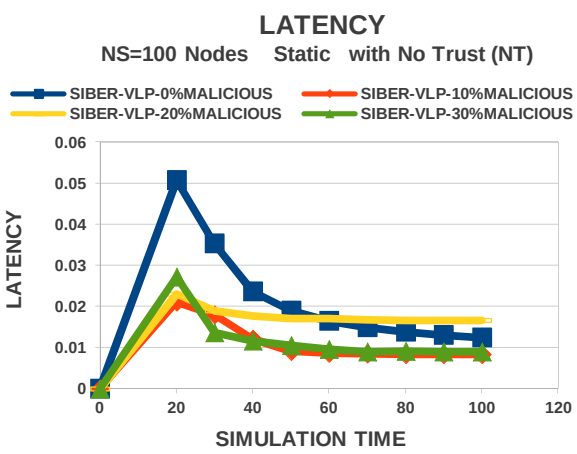


Fig. 5c) Latency vs. Time (Static 100 nodes-NT)

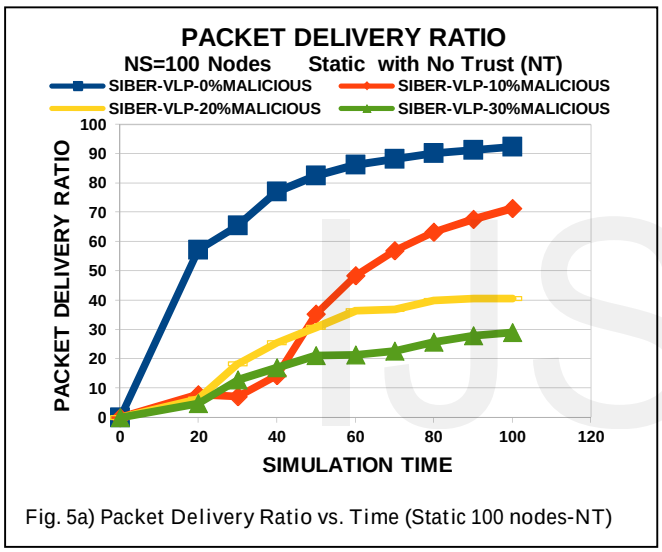


Fig. 5a) Packet Delivery Ratio vs. Time (Static 100 nodes-NT)

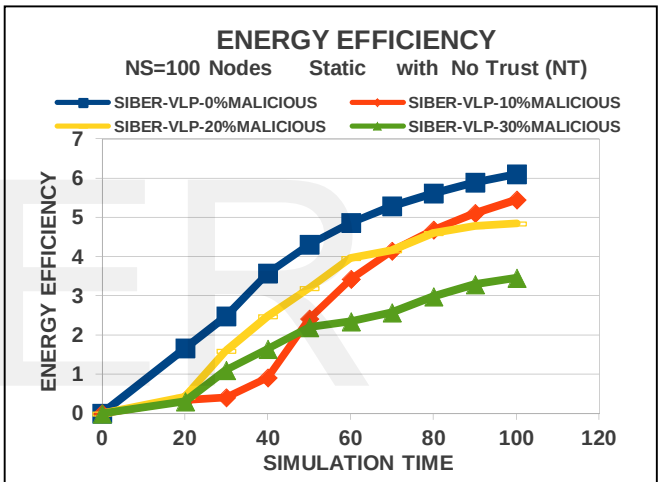


Fig. 5d) Energy Efficiency vs. Time (Static 100 nodes-NT)

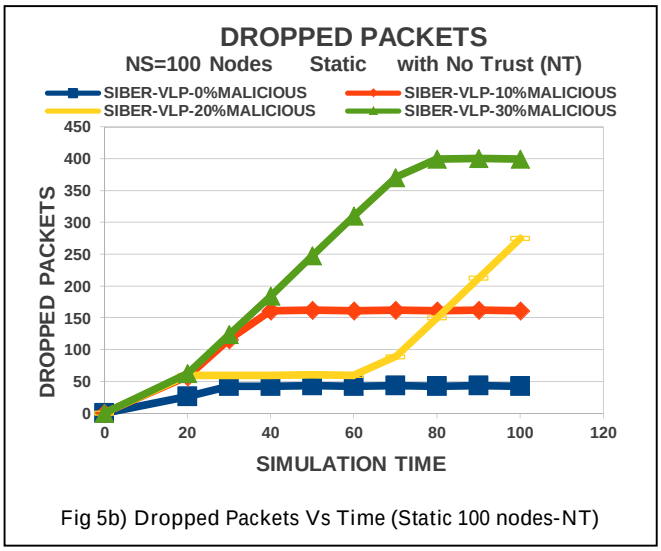


Fig 5b) Dropped Packets Vs Time (Static 100 nodes-NT)

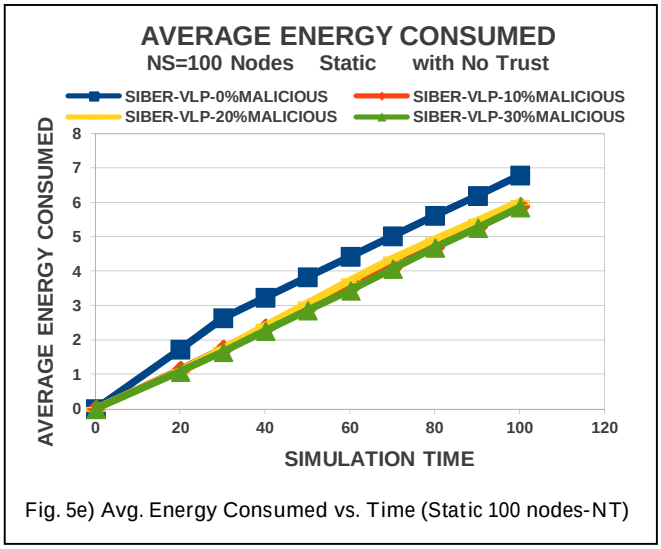


Fig. 5e) Avg. Energy Consumed vs. Time (Static 100 nodes-NT)

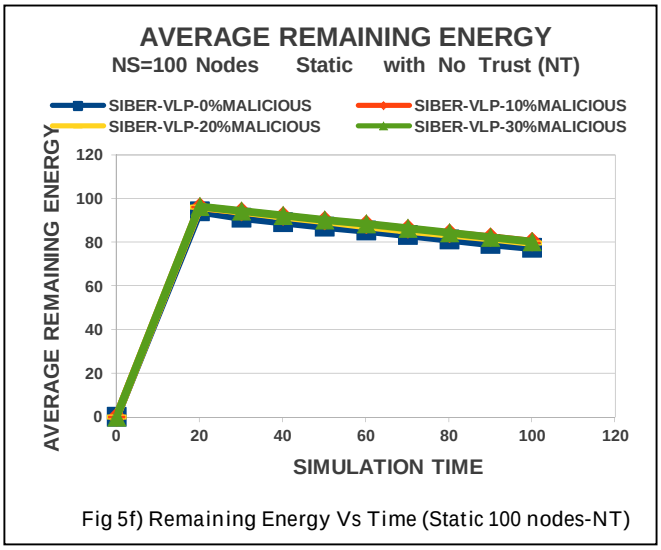


Fig 5f) Remaining Energy Vs Time (Static 100 nodes-NT)

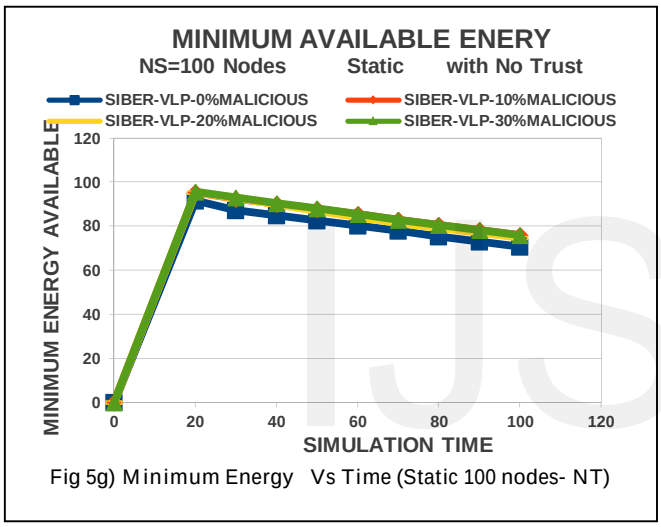


Fig 5g) Minimum Energy Vs Time (Static 100 nodes- NT)

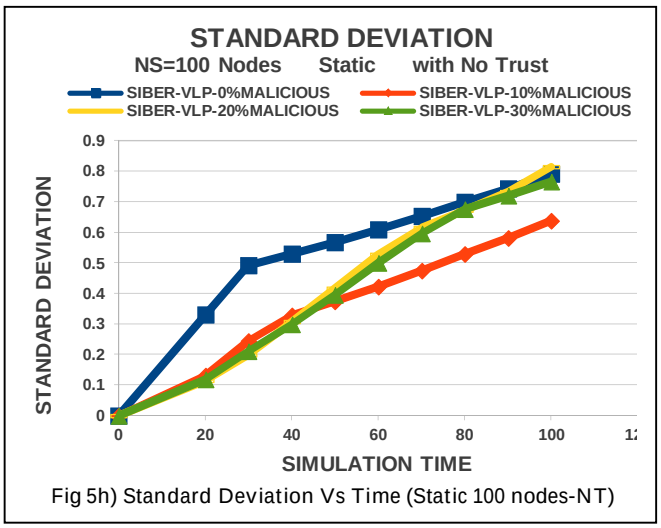


Fig 5h) Standard Deviation Vs Time (Static 100 nodes-NT)

(ii) With Trust Awareness

Next we study the performance of our proposed Trust enabled routing protocol SIBER-DELTA in the presence of 10%, 20% and 30% attackers for static network size of 100 nodes.

In our model, all nodes are assigned initially equal trust rating during the initialization and setup phase. Hence, there will be some packet drops initially immediately after the initialization and setup phase as nodes encounter neighbour nodes with equal trust rating. During the first slot of the simulation period, behaviour of nodes are evaluated in Forwarding and Monitoring Interval, T_{FMI} and new trust ratings are assigned to the nodes during the UPdate Interval T_{UPI}. This process of new node rating computation and updating is further continued in all the time slots of the simulation period.

It is to be noted that our trust enabled routing protocol SIBER-DELTA shows high packet delivery ratio as clearly seen from fig 6a). SIBER-DELTA is able to achieve a high success rate of 99.51% with 10% attackers, 98.88% with 20% attackers and 98.35% with 30% attackers in the network by avoiding completely untrusted nodes and considering only trusted nodes (i.e., nodes with higher trust rating) along the paths from source to sink. Since very less number of packet drops are observed during the entire simulation, it can be concluded that SIBER-DELTA performs extremely well by detecting all malicious nodes along the paths from source to sink and preventing these untrusted nodes from packet forwarding completely to achieve higher observed success rate.

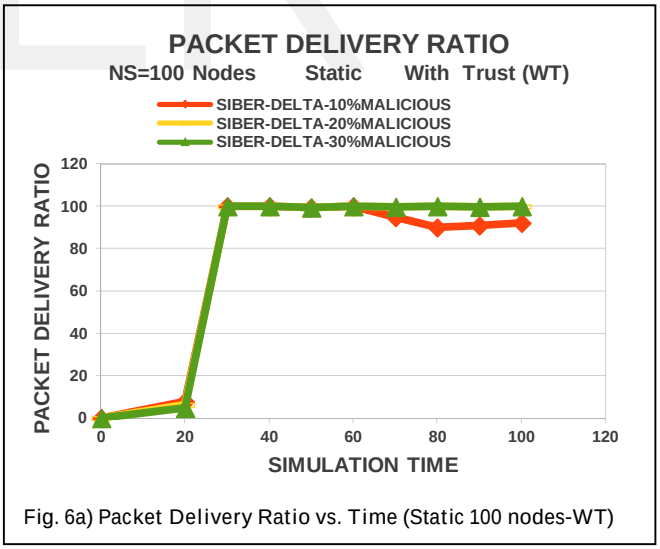
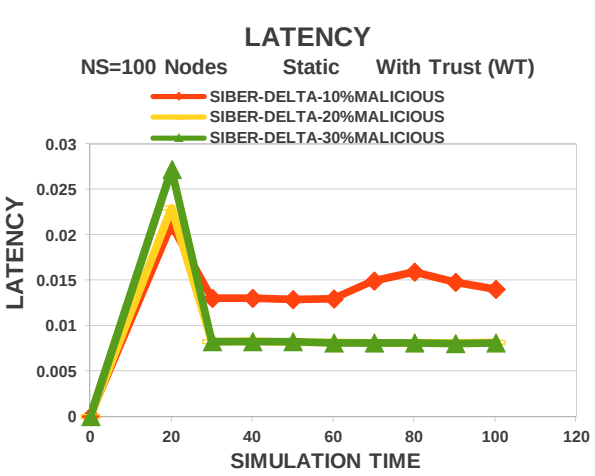


Fig. 6a) Packet Delivery Ratio vs. Time (Static 100 nodes-WT)

It is interesting to note that SIBER-DELTA with 10% attackers exhibit a significant scenario which is clearly seen after 60 secs of the simulation. In this case, as more number of packets are generated for forwarding from the source, some packets are dropped due to the non-availability of trusted nodes along some of the shorter paths within the TTL limit to the sink as these paths have only black holes which are avoided by the protocol. Hence, in such cases longer paths with hop count greater than TTL limit are selected which will

result in dropping of the packets without reaching the sink. This will result in slight reduction in packet delivery ratio, energy efficiency and further an increase in latency and energy consumption which are clearly observed in the graphs 6a) to 6f) for the case of 10% attackers after 60 secs of the simulation.



. Fig. 6b) Latency vs. Time (Static 100 nodes-WT)

Further, end to end delay or latency has been low and almost uniform due to the quality paths selected among the existing paths as shown in fig 6b) in the case of SIBER-DELTA with 20% and 30% malicious nodes. Whereas latency is slighter higher in the case of 10% attackers as it has to take longer alternate paths (i.e., paths with higher hop count) in order to avoid black holes existing in the shorter paths.

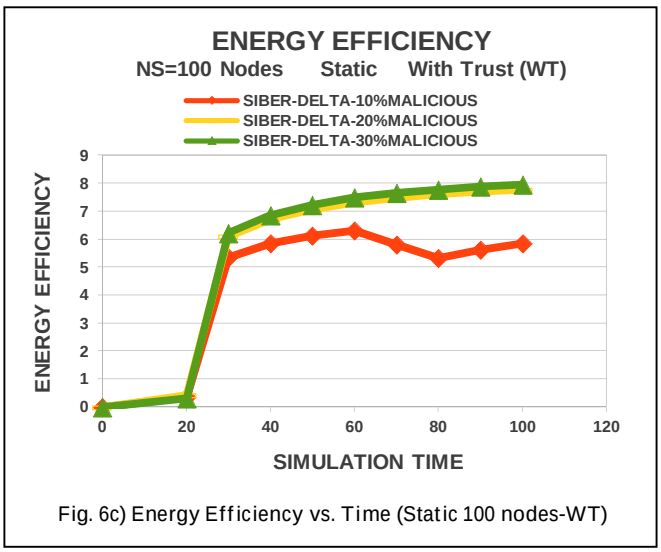


Fig. 6c) Energy Efficiency vs. Time (Static 100 nodes-WT)

As evident from Fig. 6c), SIBER-DELTA shows higher Energy Efficiency in the case of 20% and 30% attackers and slightly lower Energy Efficiency for 10% attackers as it consumes slightly higher energy due to the selection of longer alternate paths with more nodes to avoid black holes. Moreover, energy consumption has been moderate as seen in fig 6d). The Remaining Energy (fig 6e)), Minimum Energy available (fig 6f)) and Standard Deviation (fig 6g)) plots clearly indicate the energy balancing among the nodes participating in packet forwarding or delivery in the network.

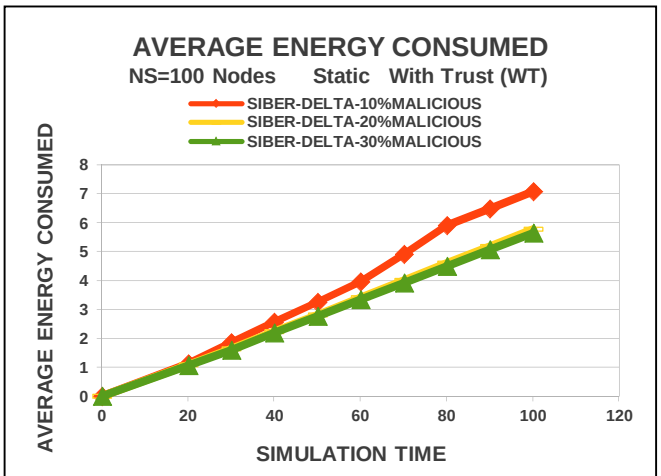
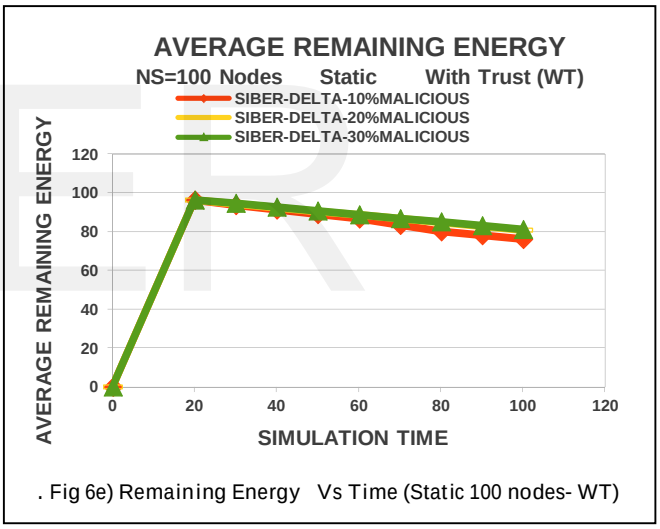


Fig. 6d) Avg. Energy Consumed vs. Time (Static 100 nodes-WT)



. Fig 6e) Remaining Energy Vs Time (Static 100 nodes- WT)

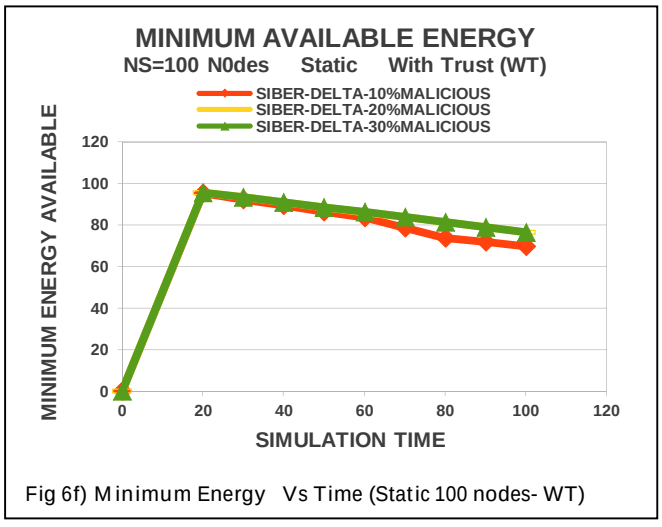


Fig 6f) Minimum Energy Vs Time (Static 100 nodes- WT)

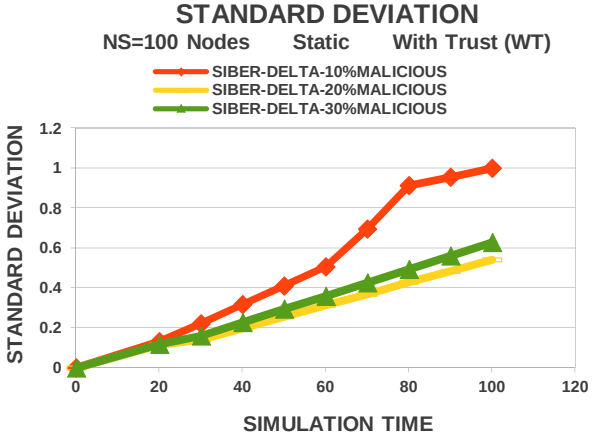


Fig 6g) Standard Deviation Vs Time (Static 100 nodes-WT)

5.4 Simulation Setup – Dynamic Scenario

The simulation parameters used in the simulation study are shown in Table 2.

Table 2 : Dynamic Scenario - Simulation Parameters

Parameter	Value
Scenario	Dynamic
Topology	Random
Number of Nodes	50, 100
Area	600 X600, 900X900
Transmission Radius	250 meters
Propagation Model	TwoRayGround
Initial Energy	30J
Transmitting Energy	1.0mW
Receiving Energy	0.5mW
Packet Size	1000 bytes
Bandwidth	11MB
Simulation Time	100 sec
Data Traffic	CBR
Data Rate	50Kbps
Mobility Model	Random Way-Point Model
Node Movement	Sink Node
Speed	5m/sec
Pause Time	15 seconds
α	2
β	2
γ	1
δ	1
ϱ	0.2

5.5 Results and Discussion - Dynamic Scenario

In dynamic scenario, all nodes except the sink node are fixed. Sink node moves at a speed of 5m/sec with a pause time of 15 secs. It is to be noted here that in static scenario, since all nodes are fixed, there will be fixed number of paths from source to sink. Where as in dynamic scenario, since destination is mobile, there will be more number of paths when compared to static environment. Here the performance of our proposed Trust aware routing protocol SIBER-DELTA in the presence of 10%, 20% and 30% attackers is studied for network size 50 and 100 nodes and the results are presented in the following sections.

5.5.1 Dynamic Scenario – Network Size = 50 Nodes with 10%, 20% and 30% Non-Forwarding attackers

The simulation results for 50-node dynamic network with 10%, 20% and 30% malicious nodes are presented in this section.

(i) Without Trust Awareness

In this simulation, first we used our developed protocol SIBER-VLP [22] without trust awareness to determine the impact of introducing 10%, 20% and 30% non-forwarding attackers on the performance of the network. As it is seen from fig. 7a), SIBER-VLP model exhibits performance degradation as malicious nodes are introduced in the network.

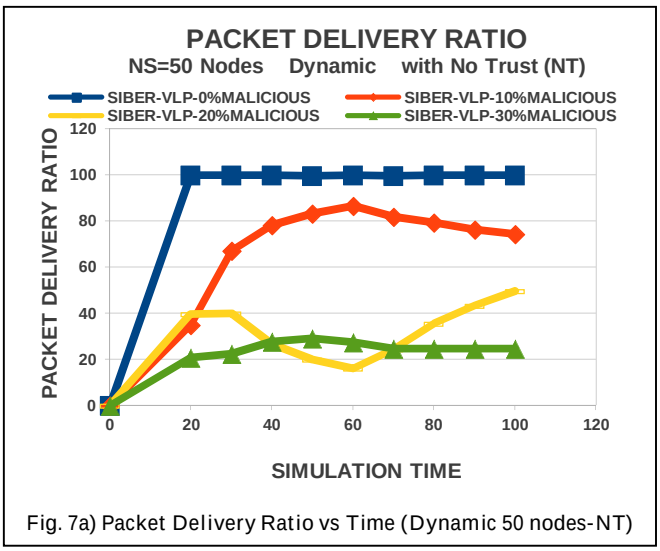


Fig. 7a) Packet Delivery Ratio vs Time (Dynamic 50 nodes-NT)

Fig. 7b) clearly shows that as the number of malicious nodes increases, we observe an increase in packet drops due to the presence of more malicious nodes in the paths selected by the ants. SIBER-VLP with 10% malicious nodes shows on an average a success rate of 73.55%, with the presence of 20% malicious nodes shows a success rate of 32.79% and with 30%

of the nodes as malicious shows very poor performance with an average success rate of 25.12%.

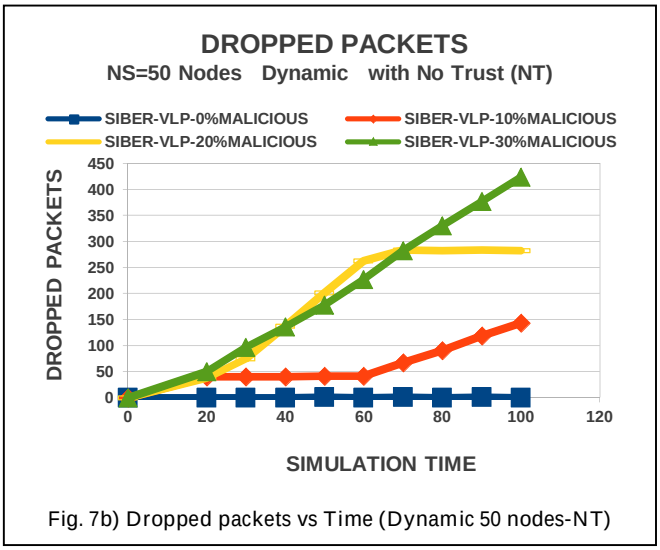


Fig. 7b) Dropped packets vs Time (Dynamic 50 nodes-NT)

As far as Energy efficiency is concerned (fig 7c)), Energy Efficiency of SIBER-VLP with malicious nodes decreases based on the number of malicious nodes or attackers in the network. When compared to SIBER-VLP without malicious nodes, Energy Efficiency decreases sharply with 25.87% decrease for 10% attackers, 66.32% decrease for 20% attackers and followed by a high reduction of 71.17% for 30% attackers as large number of packets are not delivered to the destination due to the presence of more attackers along the path to the sink.

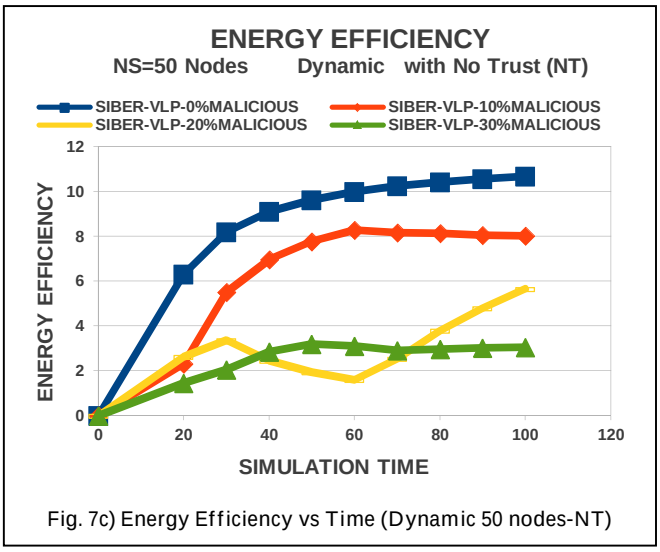


Fig. 7c) Energy Efficiency vs Time (Dynamic 50 nodes-NT)

As evident from figure 7d), SIBER-VLP with no malicious nodes uses high quality paths having less number of hops, thereby reducing the end to end delay. It is clearly seen that latency increases initially with the introduction of attackers as it takes more time to send packets to the sink at the start of the simulation due to large network size. But later as the packet drops increase due to the presence of malicious nodes in selected paths, it transmits less number of packets to the sink but selecting better quality alternate paths with less number of hops to attain energy balancing, in effect decreasing the latency.

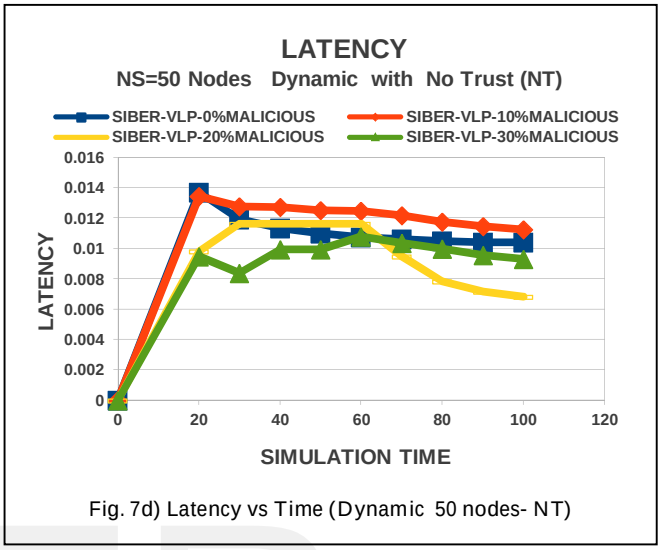


Fig. 7d) Latency vs Time (Dynamic 50 nodes- NT)

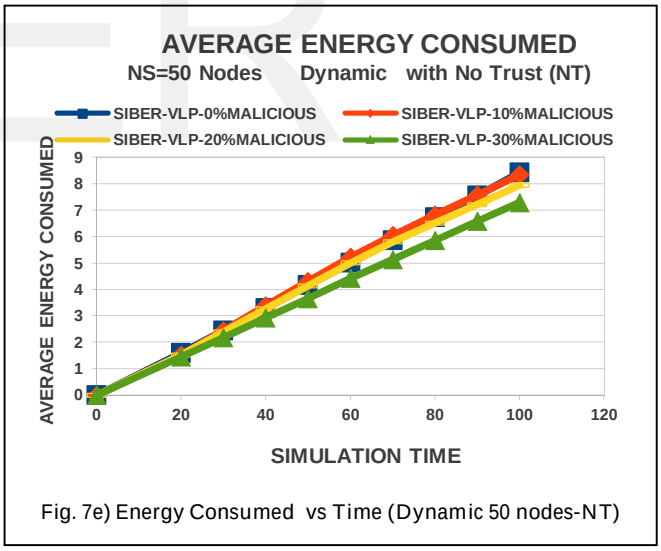


Fig. 7e) Energy Consumed vs Time (Dynamic 50 nodes-NT)

As shown in figs. 7e), with the introduction of more and more attackers, due to the presence of less number of paths to the sink and energy balancing among the nodes along the existing paths, the energy consumption is not that high when compared to SIBER-VLP with no malicious nodes.

It is to be noted that SIBER VLP with no malicious nodes should consume little higher energy (which is also seen in fig 7e)) as it achieves higher packet delivery ratio with more number of nodes along good quality paths participating in packet forwarding without any hindrance. Moreover, remaining energy and minimum available energy will also be

at a slightly higher value due to less delivery of packets to the destination as evident from fig 7f) and fig 7g) with lower standard deviation (fig 7h)).

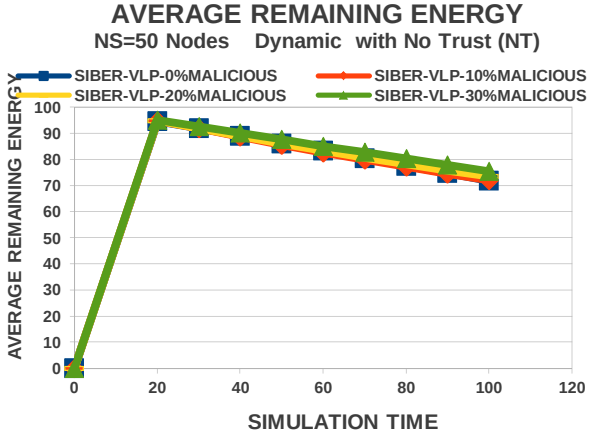


Fig. 7f) Remaining Energy vs. Time (Dynamic 50 nodes-NT)

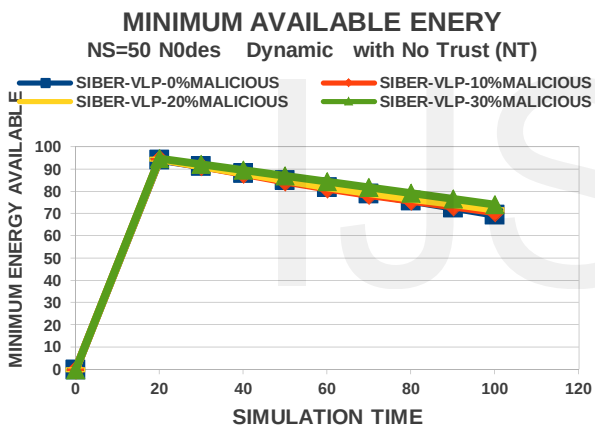


Fig. 7g) Minimum Energy vs. Time (Dynamic 50 nodes-NT)

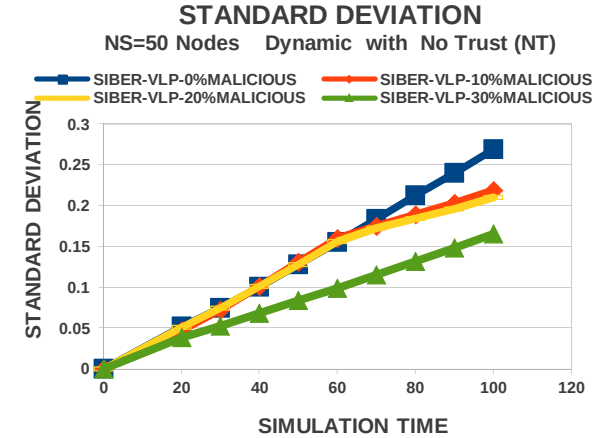


Fig. 7h) Standard Deviation vs Time (Dynamic 50 nodes-NT)

(ii) With Trust Awareness

In this section, we present the performance evaluation of our proposed trust aware routing protocol, SIBER-DELTA in the presence of 10%, 20% and 30% attackers for dynamic network size of 50 nodes.

In our model, all nodes are assigned initially equal trust rating during the initialization and setup phase. Hence, there will be some packet drops initially immediately after the initialization and setup phase as nodes encounter neighbour nodes with equal trust rating. During the first slot of the simulation period, behaviour of nodes are evaluated in Forwarding and Monitoring Interval, T_{FMI} and new trust ratings are assigned to the nodes during the UPdate Interval T_{UPI}. This process of new node rating computation and updating is continued in all the slots of the simulation period.

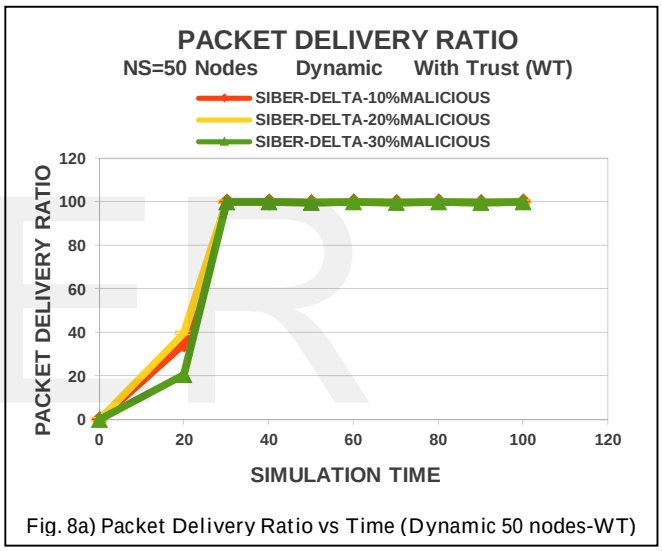
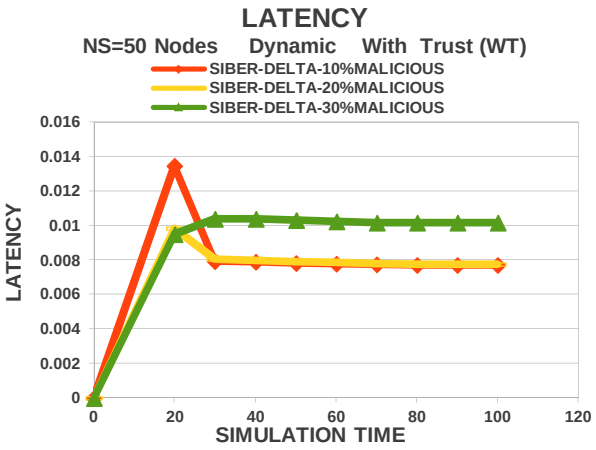


Fig. 8a) Packet Delivery Ratio vs Time (Dynamic 50 nodes-WT)

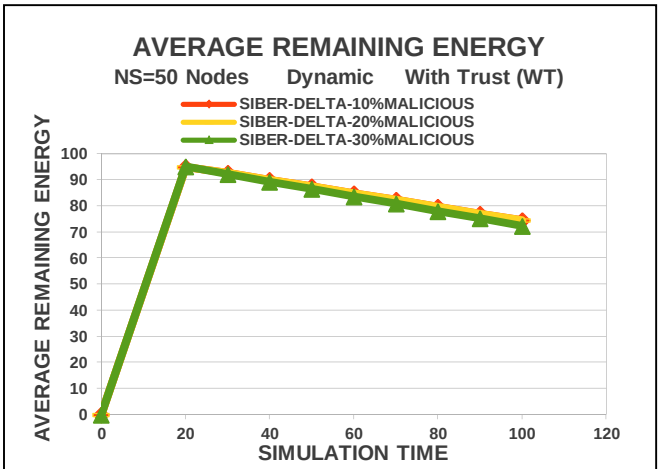
It is clearly seen from fig. 8a) that SIBER-DELTA model with trust implementation exhibits high packet delivery ratio. By avoiding completely untrusted nodes and considering only trusted nodes (i.e., nodes with higher trust rating) along the paths from source to sink, SIBER-DELTA is able to achieve a high success rate of 92.67% with 10% attackers, 93.20% with 20% attackers and 91.09% with 30% attackers in the network. Since very less number of packet drops are observed during the entire simulation, it can be concluded that SIBER-DELTA performs extremely well by detecting all malicious nodes along the paths from source to sink and preventing these untrusted nodes from packet forwarding completely to achieve higher observed success rate.

Further, end to end delay or latency has been low and almost uniform due to the quality paths selected among the existing paths as shown in fig 8b) in the case of SIBER DELTA with 10% and 20% malicious nodes. Whereas latency is

slighter higher in the case of 30% attackers as it has to take longer alternate paths (i.e., paths with higher hop count) in order to avoid black holes existing in the shorter paths.



. Fig. 8b) Latency vs Time (Dynamic 50 nodes- WT)



. Fig. 8e) Remaining Energy vs. Time (Dynamic 50 nodes-WT)

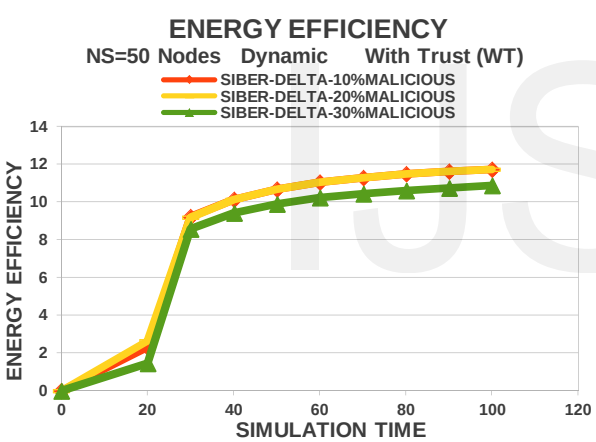


Fig. 8c) Energy Efficiency vs Time (Dynamic 50 nodes-WT)

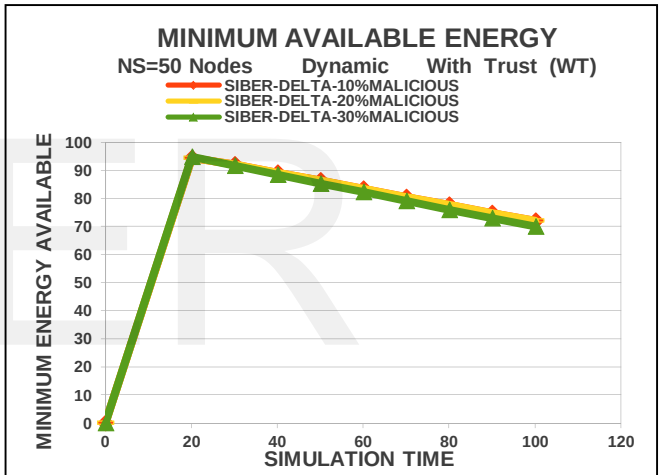


Fig. 8f) Minimum Energy vs. Time (Dynamic 50 nodes-WT)

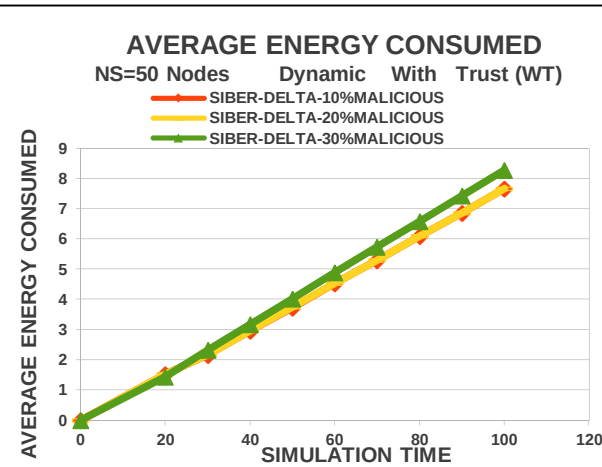


Fig. 8d) Energy Consumed vs Time (Dynamic 50 nodes-WT)

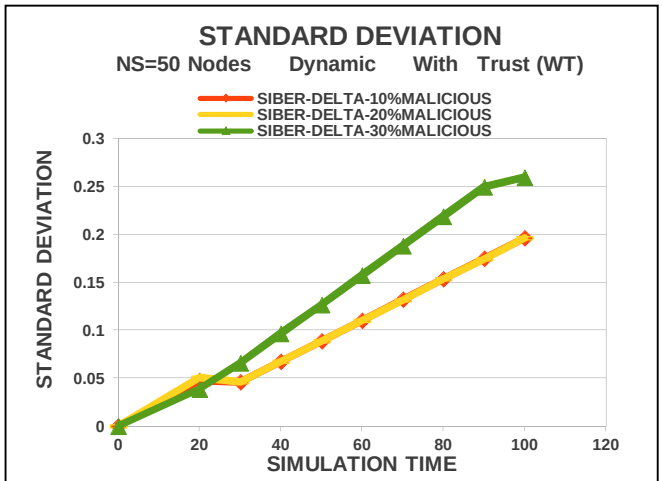


Fig. 8g) Standard Deviation vs Time (Dynamic 50 nodes-WT)

As evident from Fig. 8c), SIBER-DELTA shows higher Energy Efficiency in the case of 10% and 20% attackers and slightly lower Energy Efficiency for 30% attackers as it consumes slightly higher energy due to the selection of longer alternate paths with more nodes to avoid black holes. Moreover, energy consumption has been moderate as seen in fig 8d). The Remaining Energy (fig 8e)), Minimum Energy available (fig 8f)) and Standard Deviation (fig 8g)) plots clearly indicate the energy balancing among the nodes participating in packet forwarding or delivery in the network.

5.5.2 Dynamic Scenario – Network Size = 100 Nodes with 10%, 20% & 30% Non-Forwarding attackers

In this section, we present the simulation results for 100-node dynamic network with 10%, 20% and 30% malicious nodes.

(i) Without Trust Awareness

First, we simulated our protocol SIBER-VLP without trust awareness to study the effect on the performance in the presence of 10%, 20% and 30% non-forwarding attackers in the network. As malicious nodes are introduced in the network, the performance of SIBER-VLP degrades as shown in fig 9a). It is clearly seen from figure 9b) that the packet drops increase enormously with the increased presence of malicious nodes in the paths selected by the ants to the sink. As evident from fig 9a), SIBER-VLP with 10% attackers shows a decreased average success rate of 55.02%, with 20% attackers the packet delivery ratio reduces to 37.71% and with 30% attackers, it further reduces to a very low value average of 8.09%. Overall success rate degrades drastically with the percentage increase of malicious nodes in the network when compared to network without non-forwarding attackers.

It is clearly seen from fig 9c) that latency increases initially with the introduction of attackers as it takes more time to send packets to the sink at the start of the simulation due to large network size. But later as the packet drops increase due to the presence of malicious nodes in selected paths, it transmits less number of packets to the sink but selecting better quality alternate paths with less number of hops to attain energy balancing, in effect decreasing the latency. SIBER-VLP with no malicious nodes shows reduced end to end delay as it uses high quality paths having less number of hops.

It is observed in fig 9d) that the Energy Efficiency of SIBER-VLP with malicious nodes decreases as percentage of attackers increase in the network. When compared to SIBER-VLP without malicious nodes, Energy Efficiency decreases sharply with 27.54% decrease for 10% attackers, 44.07% decrease for 20% attackers and followed by a high reduction of 83.26% for 30% attackers as large number of packets are not delivered to the destination due to the presence of more attackers along the path to the sink.

Due to the presence of less number of paths to the sink and energy balancing among the nodes along the existing paths, the energy consumption is not that high in the case of SIBER-VLP with malicious nodes as shown in fig. 9e).

It is to be noted that SIBER VLP with no malicious nodes consumes little higher energy as it achieves higher packet delivery ratio with more number of nodes along good quality paths participating in packet forwarding without any hindrance. Moreover, Remaining Energy and Minimum Energy will also be at a slightly higher value due to less delivery of packets to the destination as evident from fig 9f) and fig 9g) with lower standard deviation (fig 9h)).

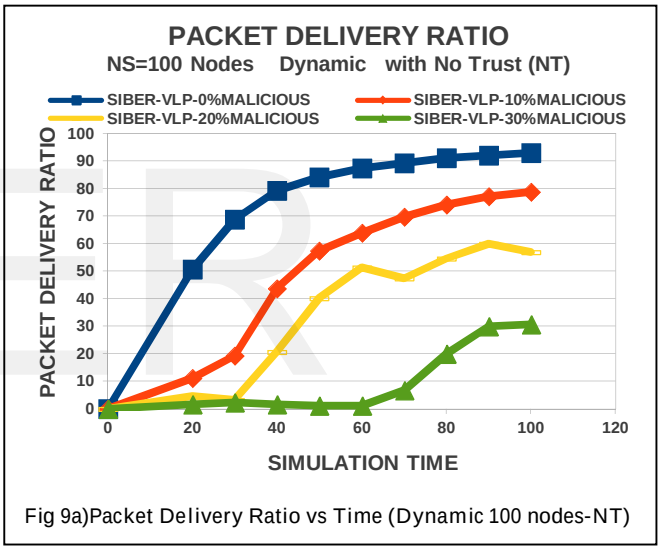
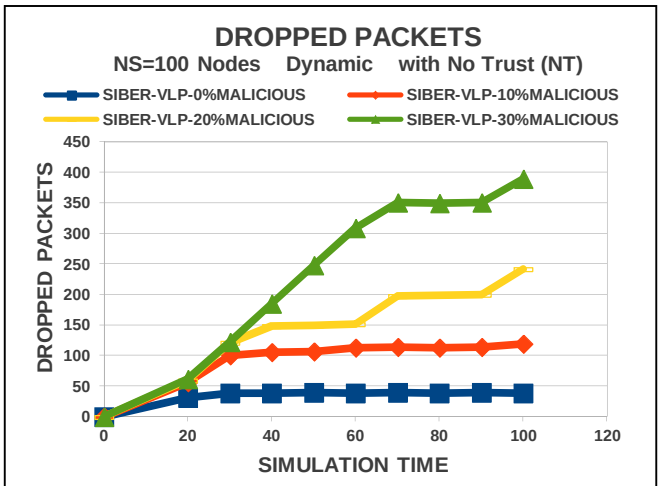


Fig 9a)Packet Delivery Ratio vs Time (Dynamic 100 nodes-NT)



. Fig. 9b) Dropped packets vs Time (Dynamic 100 nodes-NT)

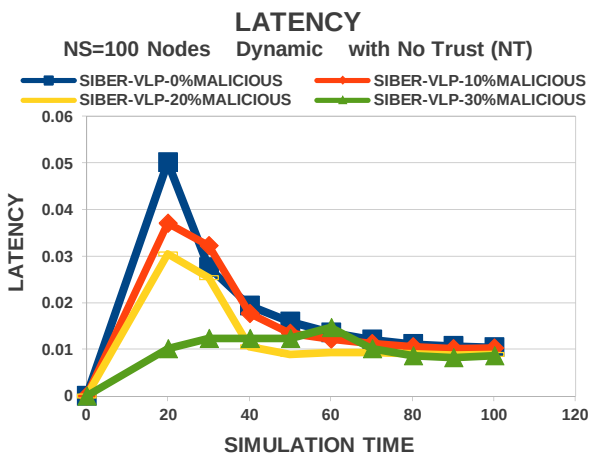


Fig. 9c) Latency vs Time (Dynamic 100 nodes-NT)

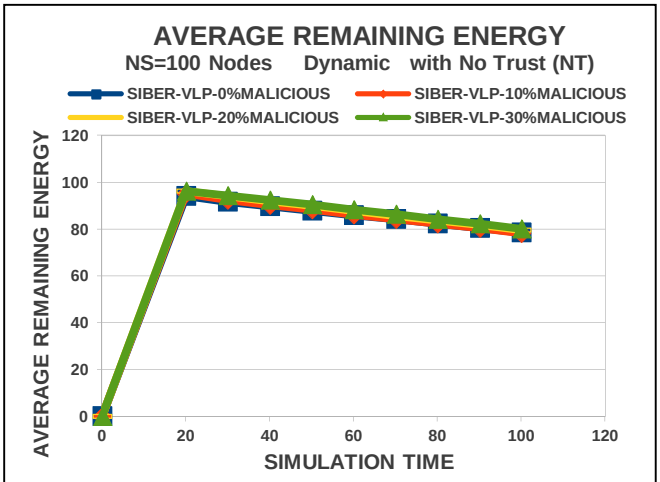


Fig. 9f) Remaining Energy vs Time (Dynamic 100 nodes-NT)

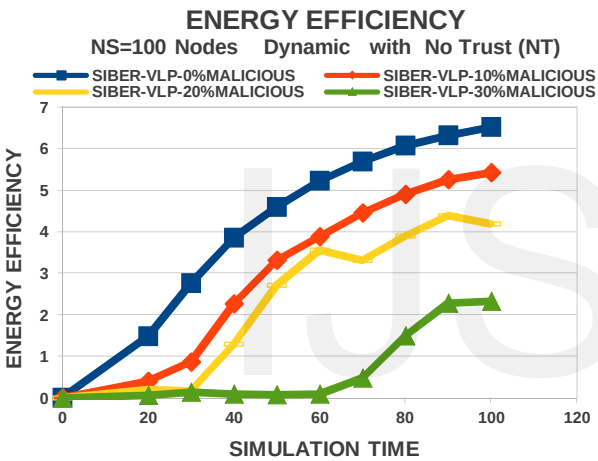


Fig. 9d) Energy Efficiency vs Time (Dynamic 100 nodes-NT)

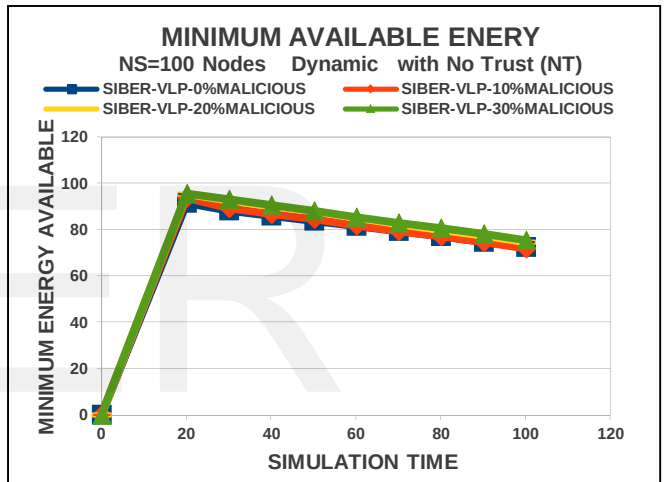


Fig. 9g) Minimum Energy vs Time (Dynamic 100 nodes-NT)

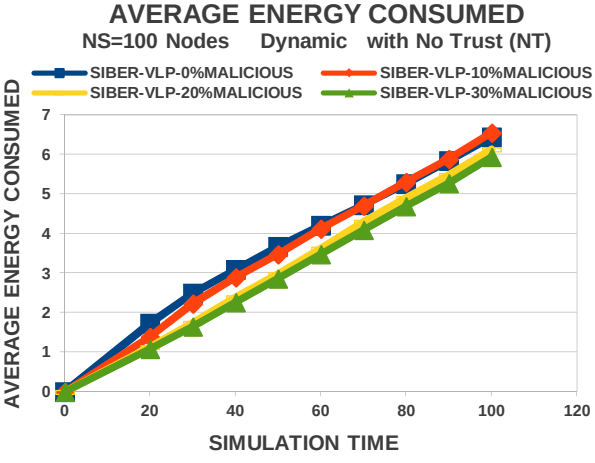


Fig. 9e) Energy Consumed vs Time (Dynamic 100 nodes-NT)

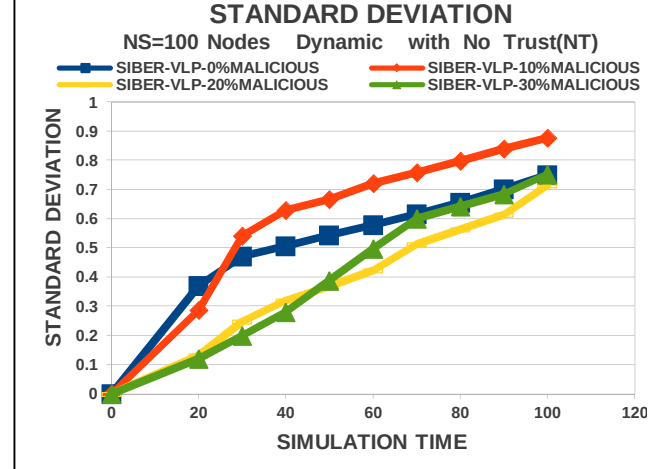


Fig. 9h) Standard Deviation vs Time (Dynamic 100 nodes-NT)

(ii) With Trust Awareness

Next we present the performance evaluation of our proposed trust enabled routing protocol, SIBER-DELTA in the presence of 10%, 20% and 30% attackers for dynamic network size of 100 nodes.

In our model, all nodes are assigned initially equal trust rating during the initialization and setup phase. Hence, there will be some packet drops initially immediately after the initialization and setup phase as nodes encounter neighbour nodes with equal trust rating. During the first slot of the simulation period, behaviour of nodes are evaluated in Forwarding and Monitoring Interval, T_{FMI} and new trust ratings are assigned to the nodes during the UPdate Interval T_{UPI}. This process of new node rating computation and updating is further continued in all the time slots of the simulation period.

It is to be noted that our trust enabled routing protocol SIBER-DELTA shows high packet delivery ratio as clearly seen from fig 10a). SIBER-DELTA is able to achieve a high success rate of 79.17% with 10% attackers, 81.10% with 20% attackers and 87.39% with 30% attackers in the network by avoiding completely untrusted nodes and considering only trusted nodes (i.e., nodes with higher trust rating) along the paths from source to sink. Since very less number of packet drops are observed during the entire simulation, it can be concluded that SIBER-DELTA performs extremely well by detecting all malicious nodes along the paths from source to sink and preventing these untrusted nodes from packet forwarding completely to achieve higher observed success rate.

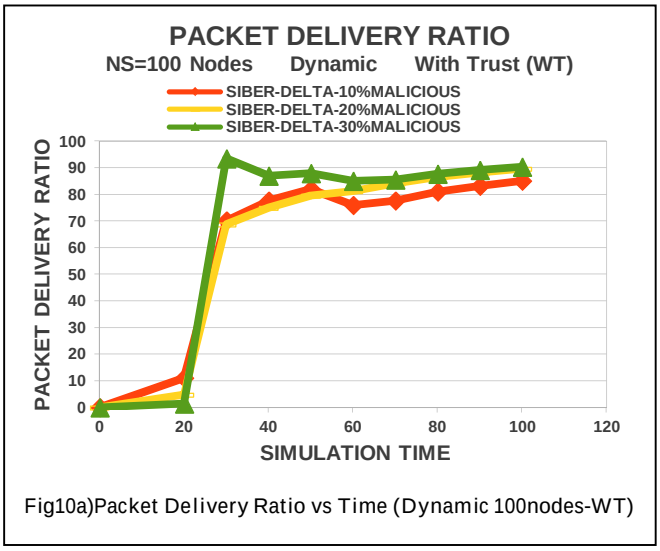


Fig10a)Packet Delivery Ratio vs Time (Dynamic 100nodes-WT)

It is interesting to note that SIBER-DELTA with 10% attackers exhibit a significant scenario which is clearly seen after 60 secs of the simulation. In this case, as more number of packets are generated for forwarding from the source, some packets are dropped due to the non-availability of trusted nodes along some of the paths to the sink as these paths have only black holes which are avoided by the protocol. This will result in slight reduction in packet delivery ratio, energy efficiency and further an increase in latency and energy consumption which are clearly observed in the graphs in figs. 10 a) to 10f) for the case of 10% attackers after 60 secs of the simulation.

Further, end to end delay or latency has been low and almost uniform due to the quality paths selected among the existing paths as shown in fig 10b) in the case of SIBER DELTA with 20% and 30% malicious nodes. Whereas latency is slighter higher in the case of 10% attackers as it has to take longer alternate paths (i.e., paths with higher hop count) in order to avoid black holes existing in the shorter paths.

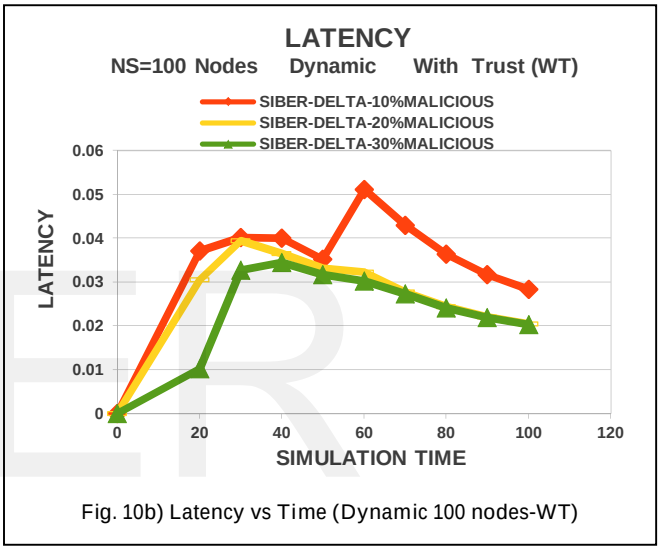


Fig. 10b) Latency vs Time (Dynamic 100 nodes-WT)

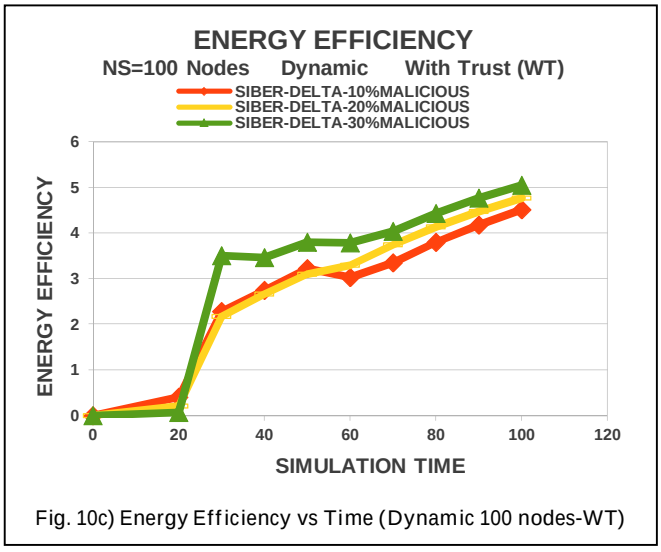


Fig. 10c) Energy Efficiency vs Time (Dynamic 100 nodes-WT)

As evident from Fig. 10c), SIBER DELTA shows higher Energy Efficiency in the case of 20% and 30% attackers and slightly lower Energy efficiency for 10% attackers as it

consumes slightly higher energy due to the selection of longer alternate paths with more nodes to avoid black holes.

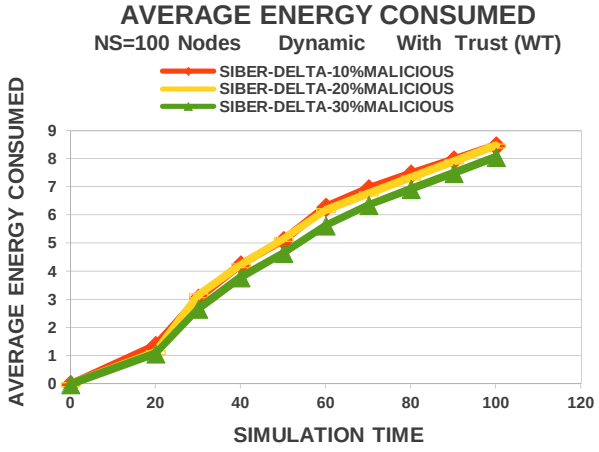


Fig. 10d) Energy Consumed vs Time (Dynamic 100 nodes-WT)

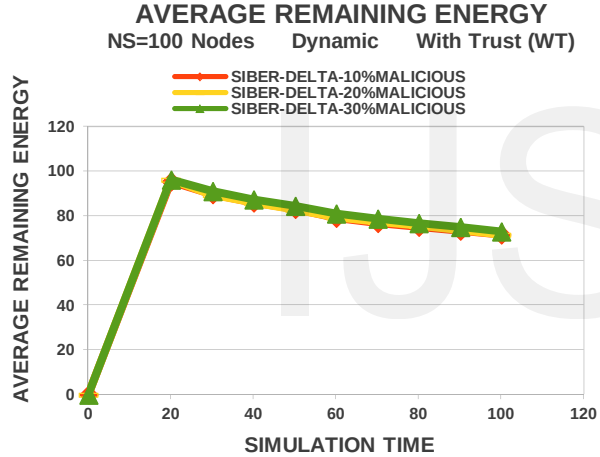


Fig. 10e) Remaining Energy vs Time (Dynamic 100 nodes-WT)

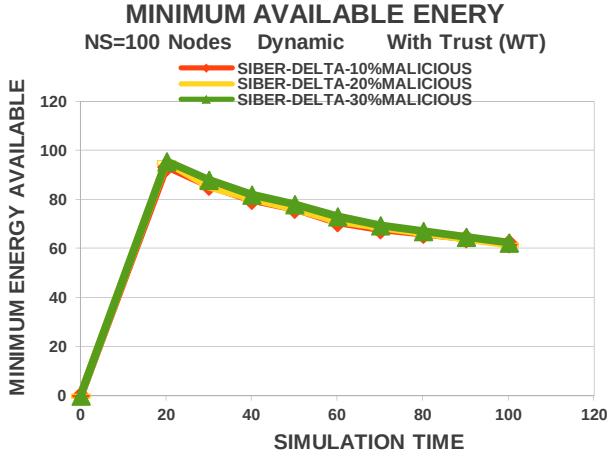


Fig. 10f) Minimum Energy vs Time (Dynamic 100 nodes-WT)

Moreover, energy consumption has been moderate as seen in fig 10d). The Remaining Energy (fig 10e)), Minimum Energy available (fig 10f)) and Standard Deviation (fig 10g)) plots clearly indicate the energy balancing among the nodes participating in packet forwarding or delivery in the network.

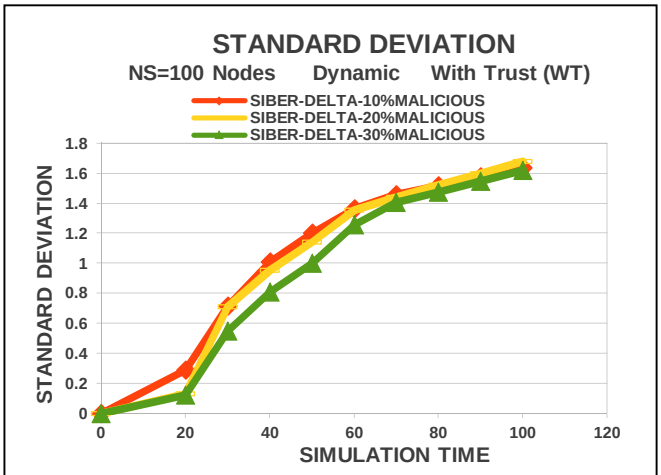


Fig.10g) Standard Deviation vs Time (Dynamic 100 nodes-WT)

6 Conclusion

In this paper, we have presented our proposed model SIBER-DELTA, Swarm Intelligence Based Efficient Routing with Distance, Energy, Link quality and Trust Awareness. In SIBER-DELTA, routing decisions are based on a weighted routing cost function which incorporates Trust, Remaining Energy, Distance, and Link quality attributes to choose the best next hop for the routing operation, thus allowing for better load balancing and network lifetime extension. The performance evaluation of our proposed Trust-Aware Routing protocol was carried out using NS-2 simulator and compared with the SIBER-VLP protocol without trust awareness by considering both static and dynamic scenarios with varying network sizes. Our simulation results indicate that SIBER-DELTA performs extremely well in detecting non-forwarding attacks and avoiding all malicious nodes from participating in packet forwarding, thereby achieving higher Packet Delivery Ratio, greater Energy Efficiency and lower Latency when compared to SIBER-VLP without trust awareness.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey", *Computer* Networks, vol. 38(4), pp. 93–422, 2002.

[2] A. R. Naseer, I.K. Maarouf , and M. Ashraf, "Routing Security in Wireless Sensor Networks", Book Chapter published in Handbook of Research on Wireless Security, Publisher: Idea Group Reference, USA, 2008, ISBN – 13:9781599048994, pp.582-616.

[3] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003.

[4] A. R. Naseer, "Reputation System based Trust-Enabled Routing for Wireless Sensor Networks", published in Handbook of Research on Wireless Sensor Networks, INTECH Open Access Publisher, USA, 2012.

[5] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation systems: Facilitating trust in internet interactions," Comm. of the ACM, vol. 43, no. 12, pp. 45–48, 2000.

[6] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Comm. Surveys & Tutorials, vol. 3, no. 4, 2000.

[7] Bonabeau, M. Dorigo, and G. Theraulaz (1999). "*Swarm intelligence: From natural to artificial systems*", Oxford University Press, London, UK, pp. 1-278, 1999

[8] M. Dorigo, and G.A. Di Caro (1998). "AntNet: Distributed stigmergetic control for communications networks", *Journal of Artificial Intelligence Research*. vol. 9, pp. 317–365, 1998.

[9] I. K. Maarouf and A. R. Naseer, "SNARE : Sensor Node Attached Reputation Evaluator", in Proceedings of IEEE/ACM 2nd International CONEXT conference, Dec. 4-7, 2006, Lisboa, Portugal.

[10] I. K. Maarouf and A. R. Naseer, "WSNodeRater: An optimized Reputation System Framework for Security Aware Energy Efficient Geographic Routing in WSNs", in Proceedings of ACS/IEEE International Conference on Computer Systems and Applications, AICCSA '2007, May 13-16, 2007 Amman, Jordan

[11] A. R. Naseer, I.K. Maarouf, U. Baroudi, , "Efficient Monitoring Approach for Reputation System based Trust-aware Routing in Wireless Sensor Networks", International Journal of IET Communications – Wireless Adhoc Networks, May 2009, Volume 3, Issue 5, pp. 846-858, ISSN 1751- 8628.

[12] I.K. Maarouf, U. Baroudi, A. R. Naseer, "Cautious Rating for Trust-enabled Routing in Wireless Sensor Networks", EURASIP International Journal on Wireless Communications and Networking, 2010, Volume 2, Article ID 718318, 16 pages, ISSN: 1687-1472.

[13] A. R. Naseer, "EMPIRE – Energy Efficient Trust-Aware Routing for WSN", Handbook of Research on Dynamic Ad Hoc Networking, IET Publisher, UK/USA, 2013

[14] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, pp. 66-77, October 2004.

[15] Audun Josang, Roslan Ismail, "The Beta Reputation System", 15th Bled Electronic Commerce Conference, e-Reality: Constructing the e-Economy. Bled, Slovenia, June 2002.

[16] A. Srinivasan, J. Teitelbaum and J. Wu, "DRBTS: Distributed Reputation based Beacon Trust System", 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), Indianapolis, USA, pp. 277–283, 2006.

[17] M. Krasniewski, P. Varadharajan, B. Rabeler, S. Bagchi, and Y. Hu, "TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks", Proceedings of the International Conference on Dependable Systems and Networks (DSN'05), (Yoko-hama, Japan), June 2005.

[18] Z. Yao, D. Kim, and Y. Doh. PLUS: Parameterized and localized trust management scheme for sensor networks security", In *Proc. of the 3rd IEEE Int. Conf. on Mobile Ad-hoc and Sensor Systems*, pages 437–446, Vancouver, Canada, Oct. 2006.

[19] Hu, J., Burmester, M., 2006. "LARS: a locally aware reputation system for mobile ad-hoc networks", in *44th annual ACM Southeast Regional Conference, 2006*.

[20] G. Zhan, W. Shi, and J. Deng, "TARF: A trust-aware routing framework for wireless sensor networks," in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10)*, 2010.

[21] Zhan, G., Shi, W., Deng, J., "Sensortrust - a Resilient trust model for WSNs", SenSys 2009, Proceedings of the 7th International Conference on Embedded Networked Sensor Systems , 2009

[22] V. Neelima and A. R. Naseer, "SIBER-XLP: Swarm Intelligence Based Efficient Routing Protocol for Wireless Sensor Networks with Improved Pheromone Update Model and Optimal Forwarder Selection Function", International Journal of Advanced Research, Vol. 4, issue 7, pp. 769-789, ISSN 2320-5407, 2016.

[23] V. Neelima and A. R. Naseer, "Impact of Threshold Energy Control on Energy Conservation and Balancing in Swarm Intelligence Based Efficient Routing for Wireless Sensor Networks", accepted for publication in the Procs. of World Congress on Engineering and Computer Science, WCECE2016, San Francisco, US, 19-21 Oct. 2016.

Authors Brief Profile

V. Neelima Associate Professor in the Department of Computer Science & Engineering at Jyothishmathi Institute of Technology and Science Karimnagar, Telangana State, India, Received B.Tech in Computer Science and Engineering from Bhoj Reddy Engineering College for Women affiliated to Jawaharlal Nehru Technological University Hyderabad (JNTUH) in 2004, M.Tech in Computer Science and Engineering from Ramappa Engineering College affiliated to JNTUH in 2010, Currently pursuing her Ph.D. from JNTUH in the area of Security for Wireless Sensor Networks, member of several National and International Professional Bodies - member of IEEE Computer Society, USA, member of IAENG, UK. Her Research interests include swarm intelligence based efficient routing in wireless sensor networks, energy balancing & conservation in WSN, trust aware routing and security aspects of wireless sensor networks.

Dr A. R. Naseer Principal & Professor of Computer Science & Engineering at Jyothishmathi Institute of Technology & Science (JITS), affiliated to Jawaharlal Nehru Technological University (JNTU), Hyderabad, India, Received Ph.D. (Computer Science & Engineering) from Indian Institute of Technology (IIT), Delhi, India (1996) and M. Tech. (Industrial Electronics) from NITK Surathkal, Karnataka state, India(1985) securing I Rank of Mangalore University, held several higher responsible academic/ administrative positions & served as Chairman & Member of several University Boards & Committees in India and abroad since 1986, Recipient of several awards & honors – IEEE Best Student Paper award (1994), Distinguished Teacher award(2004-2007), Life-time Education Achievement award, Asia Pacific International award for Education Excellence at Tashkent, Indo-Nepal unity award, Gold Star Asia

International award for Education Excellence, Indo-Nepal Ratan award at Kathmandu Nepal, Best Educationist award, Bharat Shiksha Ratan award, Jewel of India award (Man of the year award) for Education Excellence, Mother Teresa Excellence award, Rajiv Gandhi Excellence award, Indira Gandhi Shiksha Shiromani award, Bharat Excellence Award, Global Achievers Award For Talented Personalities, Academic Leadership Award, Best Academic Administrator Award, and Eminent Educationist award, Profile included in Marquis USA Who's Who in the World 2013, 2014, 2015 and Marquis USA Who's Who in Science & Engineering in the World 2016, Member of several National and International Professional Bodies – Senior Member of IEEE Computer Society, USA, IEEE Communications Society, USA, Member of IAENG, UK, Life Member of Indian Society for Technical Education (ISTE), Life Member of Computer Society of India (CSI), Member of VLSI Society of India (VSI), Areas of research interests include Security in WSN & MANET, Cross-Layer Architecture for Wireless Networks, Data Mining & Warehousing, Bio-inspired Computing, Swarm Intelligence, Cryptography & Network Security, Computer Architecture, Multi-Core Architectures, Design Automation and FPGA based Synthesis, Parallel & Distributed processing.