*Sādhanā* Vol. 41, No. 11, November 2016, pp. 1261–1274
DOI 10.1007/s12046-016-0557-9


# Context sensitive trust based geographic opportunistic routing in mobile ad hoc networks

A RAJESH[1,*] and N MOHAN KUMAR[2]

[1]Department of Computer Science and Engineering, S.K.P. Engineering College, Thiruvannamalai 606 611, India
[2]Department of Electronics and Communication Engineering, S.K.P. Engineering College, Thiruvannamalai 606 611, India
e-mail: svishnuraj7@yahoo.co.in; nmkphdju@gmail.com

MS received 29 June 2015; revised 3 February 2016; accepted 29 April 2016

**Abstract.** Position based opportunistic routing (POR) is a stateless, robust, and reliable geographic routing protocol in Mobile AdHoc NETwork (MANET). The opportunistic routing embraces broadcast property of wireless channels and utilizes it for opportunistic forwarding. Both the malicious node behavior and the backup nodes' behavior are equally treated as malicious in the existing misbehavior detection mechanisms. Hence, incorporating a general trust model in POR is not combative with routing attacks. It is necessary to determine whether the misbehavior is likely a result of malicious activity or due to the backup scenario of opportunistic forwarding. On the other hand, if context-sensitive trust information is available on every node, it ensures a fair decision making and also supports secured routing in an opportunistic approach. This work investigates the utilization of context attributes along with generic trust model to allow POR for secure and reliable data forwarding. This paper introduces context-sensitive trust for choosing the data forwarding node in POR (CPOR) to assist opportunistic routing in selecting the trusted optimal data forwarding node and to cope with both security and reliability of communications. The proposed work exercises both coarse- and fine-grained trust evaluation to strengthen the trustworthiness. The coarse-grained trust measure includes positive progress per hop and behavioral attribute of the nodes in terms of routing service. The fine-grained trust evaluation differs the opportunistic routing environment from the adverse scenarios and aids the source node such that it builds a highly trusted positive progress set using contextual attributes. The fine-grained trust evaluation deduces the ideal contextual information such as the link quality, battery energy, and the backup service to determine the accurate trust value of nodes. As a result, it involves optimal routes and enables CPOR to maintain the routing performance equal to the POR even in the presence of malicious nodes in the network. The simulation results demonstrate that the packet delivery ratio of the proposed context-aware trust model is substantially high even when 50% of the total nodes are found malicious and outperforms the trust-aware opportunistic routing protocol (TAOR).

**Keywords.** POR; contextual attributes; behavioral attributes; trust; context-sensitive trust model.

## 1. Introduction

The efficiency and robustness of the opportunistic routing attract many recent applications in wireless networks. Position based opportunistic routing (POR) is the latest geographic routing protocol based on the opportunistic forwarding in Mobile AdHoc NETwork (MANET) [1, 2]. The opportunistic routing forwards the data packets similar to multicast in which several nodes cache the data packet using media access control (MAC) interception. The source node determines a forwarder list based on its location information and the list gets inserted into the IP header. When the main forwarder fails to transmit the data packet the backup nodes take a turn to forward it. The attacking nodes disrupt the POR routing process with their malicious activities. It is likely that the main forwarder and/or a backup candidate may launch an attack to degrade the performance of the routing process. Moreover, it is not so easy to differentiate the attacker and the activities of the backup nodes in opportunistic routing.

Trust is the key factor to strengthen the robustness of the POR in the presence of malicious nodes. As per the POR, the backup nodes drop the packet without re-forwarding, when the main forwarding candidate transmits the same packet. While computing the trust value, a backup node appears to be an adversarial node due to activities such as

*For correspondence

the packet delay and the packet drop. As a result, it reduces the trust value of a backup node. This scenario leads to misclassification of a genuine node as a malicious one and gets eliminated from the list of forwarding candidates. It implies that the general trust model is not directly applicable to opportunistic routing. Thus, the use of context attributes [3–5] with generic trust model becomes necessary for developing trust-based security architecture, especially in opportunistic routing. When applying the trust model, contextual information is a supplement for improving the routing decision. The incorporation of context awareness in a rapidly changing battlefield environment is inevitable. The contextual information helps to identify the soldiers who die during their service or about whose equipment is turned off, or temporary whereabouts and the exact movement of soldiers on a battlefield. Moreover, in case of disaster, mobile networks may be heavily congested due to multiple transmissions at a time. Thus, congestion probability plays an important role in disaster management. Traffic refers to vehicle mobility which indicates the vehicle speed (relative mobility) and volumes. The awareness of this context attribute tends to high-speed and high-volume safety roadways.

Thus, the proposed work extends POR with the context-aware trust model to support the highly demanding battlefield scenario. The extended POR utilizes the advantages of the stateless property of geographic routing and contextual information such as the link quality, remaining battery energy, and backup service while selecting the most trusted forwarding candidates.

- The major contribution of this work is to extend POR that builds the contextual aware trust on the generic model for detecting and preventing the malicious nodes and ensuring the most trusted nodes for data forwarding.
- The proposed work applies both coarse- and fine-grained trust evaluations to deal with the complex model of opportunistic routing, as the backup nodes in the forwarding state pretend as adversarial nodes.
- The CPOR fine tunes the coarse-grained trust value depending on behavioral attributes and position information using contextual attributes such as link quality and remaining battery energy and ensures the quality of service (QoS) routing.
- The use of backup service offline-grained trust value enables the CPOR to determine whether the misbehavior is likely a result of malicious activity or due to network conditions and ensures the security in the opportunistic routing.
- The consideration of QoS and Social interactions makes CPOR achieve an optimal balance between the reliability and the security. The performance of the CPOR is compared with the TAOR using NS2 simulator.

### 1.1 *Paper organization*

The remaining part of the paper is organized as follows: Section 2 discusses the related works. Section 3 describes the system model. Section 4 illustrates the proposed methodology for the overall functional components. Section 5 analyzes the throughput and the overhead of the proposed work. Section 6 evaluates the performance of the CPOR protocol and section 7 concludes the paper.

## 2. Related works

A complete survey and various aspects of trust management on MANET is presented in [6]. The proposal in [7] identifies context-aware trust relationships that enable the users to select the most trustworthy services. The weakness of this method is that it fails to validate and fine-tune the trust model. The paper in [8] presents the importance of context-awareness in routing to enhance the security of wireless sensor networks. It relies on the context, and it utilizes the knowledge base to extract the importance of a message through the context information. A geographic routing algorithm with context awareness detects the holes in the network [9]. This algorithm is known as HOle-Bypassing routing with Context-AwareNess (HobyCan). The HobyCan sets up several alternative paths to bypass holes in the network. The Context-aware Adaptive Routing (CAR) protocol ensures delay-tolerant routing [10]. The CAR exploits the prediction concept to route the message packets efficiently, and the nodes are used as message carriers during the network separation to reach a better delivery rate. The CAR selects the best and the suitable message carriers using prediction methods of the Kalman filter and utility theory. A trust-based decentralized security architecture meets the challenges of security management and context awareness computation [11]. This security architecture establishes suitable trust levels for any given context. SECURE and Aithe are the outcomes of the security architecture. The SECURE manages with the trust engine and the risk engine for trust management. On the other hand, Aithe gathers and manages context information from sensors. A context-aware mechanism detects selfish nodes using a context-aware inference method in a dynamic source routing (DSR) [12] and punishes the malicious and misbehaving nodes.

An approach in [13] proposed a secure routing protocol that follows a distributed trust model and the geographical routing strategy. The routing decision is based on the location, trust, and energy information. The accuracy of distributed trust model depends on both the direct and the indirect observations and also to ascertain the trust value of each neighbor node. The proposal in [14] incorporates a weighed routing cost function in geographic routing

scheme and also balances the trust and the location information, but it lacks energy awareness. The concept of context supports the trust management system in [15]. It introduces contextual fitness, a component of the computational trust and reputation (CTR) system that appends context into the loop of trust management. The notion of contextual fitness empirically optimizes the trust values in a context-aware manner.

The context-aware secure and trust framework (CAST) exploit contextual information to detect the misbehavior [16]. This algorithm supports local as well as global views. The trust value is updated based on the contextual view communication channel status, battery status, and weather condition. This method significantly reduced its communication overhead. Unlike the existing works, an approach in [17] deals with the problem of having faulty nodes in-the-air backup, and this approach is named as trust-aware opportunistic routing (TAOR) protocol. The TAOR approach uses the link delivery probability between nodes, and also the trust value that each node calculates about its neighbors to select secure next-hop nodes in the candidate set. However, this model considers only the direct trust measurement, and it lacks in defining the trust in different contexts.

The existing trust models [13–16] measure the trust value using the routing behavior, and the QoS attributes context such as location, channel status, and energy information of nodes, but for opportunistic routing, the focus on nodes' involvement in-the-air backup is essential. However, the accuracy of the estimated context-aware trust value cannot be completed with either the backup service [17] or QoS attributes context alone. The proposed work designs a context-sensitive trust model for geographic routing scheme that utilizes the advantage of QoS attribute context and also considers the backup service as social attribute context. The designed trust model tunes the trust value based on the context attributes and determines the proper QoS and social trust value of a node. This context-based information enables the proposed work to select an appropriate node as the next-hop.

## 3. System model

The wireless network is considered as a graph $G$ ($V$, $E$) in which $V$ represents a set of nodes, and $E$ represents a set of direct links. The network $G$ dynamically creates $E$ between a pair of mobile nodes. Let the total number of nodes in the network be $N$ such that $|V| = N$. Assume that each node is aware of its position and neighbor nodes accurately. The range of node connectivity is limited to one-hop and bounded by the maximum distance $R$. The geographic location of each node in $V$ is represented as here $V_X$ and $V_Y$ represent the coordinates. Consider a node $S \in V$ with the location ($S_X$, $S_Y$) and $N_S$ is a set of one-hop neighbors of $S$. Each node senses the contextual information such as the distance, link quality, and the battery status to decide the list of the forwarding candidates. Let $D_{S\text{-}NS}$ represents the distance between $S$ and the positive progress set ($P_S$). Let $BT_{Ns}$ represent the battery status of the neighbor nodes. $S$ selects its positive progress set in $N_S$, $P_S = \{1, 2, 3,\ldots,n\}$ considering the ($S_X$, $S_Y$) as a reference point.

The MANET is vulnerable to routing attacks due to the wireless medium and dynamic network topology. Consider the network $G$, it consists of the number of malicious nodes (M) among N nodes and the number of benevolent nodes $B = N-M$. It is assumed that there are two types of attacking nodes M such as selfish (SM) and misbehaving nodes (MM). The scope of SM is to save its battery energy, $BT_{SM}$ without involving in routing activities. However, MM nodes are intended to attack other nodes (B), and their activities. The proposed system enables each node to trace its 1-hop neighbors' activity by overhearing. The coarse-grained trust metric considers QoS and social trust, and these trust values are fine-tuned by considering the contextual information such as link quality, battery energy, and backup service. The highly trusted neighbors are selected as forwarding candidates for improving the routing security.

## 4. An overview of the proposed system

The context attributes needs to be of prime consideration during the design of context-aware trust model in order to understand the network dynamism. However, if the node has no willingness in routing, all the context information will not be of much help, and the context awareness mismatch remains. Thus, the CPOR builds the context information upon the general trust model which considers the routing behavior of a node. It takes into account both the routing behavior and the context attributes in routing decision, and differentiates the attackers from the normal network behavior.

The proposed CPOR protocol in wireless communications alleviates the security issues and meets the QoS requirements, by evaluating the coarse- and fine-grained trust evaluation. The CPOR distinguishes itself from the conventional POR in three aspects: (1) the CPOR not only considers the QoS trust in terms of positive progress per hop, but it also includes the social trust. The social trust utilizes the knowledge regarding the routing interactions between nodes and enables the CPOR to yield the ground truth against both the selfish and the malicious nodes in the coarse-grained trust evaluation. (2) Although the Coarse grained trust values are sufficient to observe the interactions between nodes, the CPOR may tend to miss some trusted nodes to include in the positive progress set. To make the new definition for positive progress to influence the trust formation in the opportunistic forwarding scenario, the CPOR takes into account the several contextual attributes

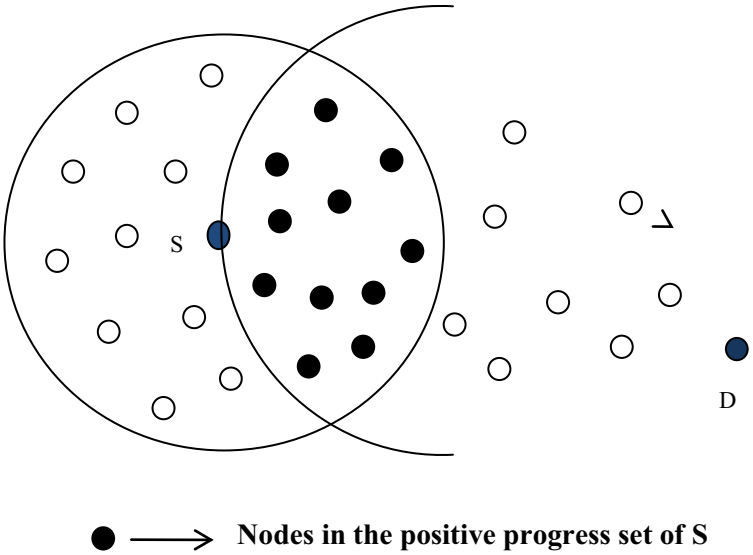


**Figure 1.** The formation of positive progress set.

like link quality, battery energy, distance, and backup service in both the QoS and social trust of fine-grained trust evaluation. (3) The CPOR considers the backup service as contextual information for social trust measurement and enables the CPOR to fit to differentiate the opportunistic routing environment from the adversary scenarios. For example, the backup candidates deny or drop the forwarding packets as per the opportunistic routing nature. Thus, the use of backup service as a proper trust evidence assists the CPOR to differentiate the backup and malicious activities and avoids it to misclassify the backup nodes as malicious nodes and influence the routing performance. Thus, the CPOR improves the security of routing while enhancing reliability in opportunistic routing.

### 4.1 *Coarse-grained trust evaluation*

Security is a critical aspect of QoS provisioning in the POR. Without protection from a security mechanism, attacks on POR could result in QoS routing malfunction. To avoid this issue, the CPOR composites both the QoS and the social trust by evaluating the coarse and the fine-grained trust evaluation. The QoS trust refers the large positive progress per hop or the capability of nodes to quickly deliver the message to the destination, whereas the social trust refers the willingness of nodes to participate honestly in the correct functioning of the CPOR. The coarse-grained trust evaluation forms the positive progress set using the QoS trust ($Q_T$) and measures the social trust ($S_T$) to the nodes in the positive progress set using interactions between the nodes.

4.1a *Coarse-grained QoS trust evaluation*: By using location information, the source node decides the positive progress set prior to measuring the $S_T$. The source node gathers the location of its entire 1-hop neighbors through periodic beacons to indicate their locations. The source node calculates its distance from the destination ($d$ ($s$, $d$)) and also the distance from each of its 1-hop neighbors to the destination ($d$ ($n$, $d$)) to form positive progress set as shown in Eq. (1). The source node forms the positive progress set ($P_S$) such that it comprises of nodes closer to the destination (D) than the source node S, keeping the location of the target node as a reference point. Figure 1 shows the formation of a positive progress set. The nodes in $P_S$ contain both social trusted and untrusted nodes.

$$P_S = \left\{ \exists (s,p) \in E \bigwedge d(p,d) < d(s,d) \right\}. \quad (1)$$

Only the neighbors in the $P_S$ are taken into account for the $S_T$ value calculation. The Social trust value is computed only for the nodes in the trusted positive progress set using routing interactions. To select the appropriate data forwarding node, the proposed work fine tunes both $Q_T$ and $S_T$ using several contextual information.

4.1b *Coarse-grained social trust evaluation*: The coarse-grained social trust value is evaluated for nodes in $P_S$ considering the behavioral attributes. All the nodes that take part in the data forwarding execute the social trust computation, and it takes into account the total number of packets sent and received without any time delay. It is essential to overhear the wireless medium and ensure the delivery of the previous packet in time to determine the probability of a node acting like a misbehaving node. If this process is certain, it is considered as a successful transmission.

The probability of a node to act as a malicious one is represented as $P_m$ as shown in Eq. (3). $P_g$ refers probability of a node to act as a genuine node. Analyze the packet

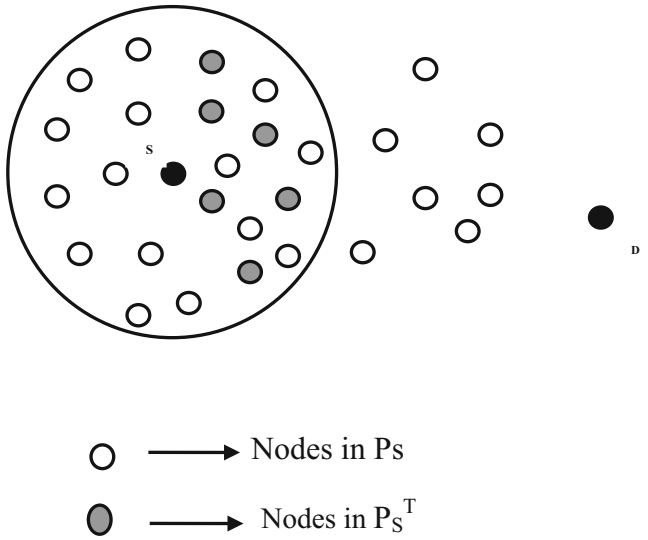


**Figure 2.** The formation of trusted positive progress set.

dropping ratio ($R_{dr}$) and packet delaying ratio ($R_{dl}$) to determine the probability of a node to act as a malicious one, where ($1 - R_{dr}$) represents the successful packet transmission, including the delayed packets.

$$P_S = (1 - P_m) \tag{2}$$

$$P_m = (1 - R_{dr}) - R_{dl}. \tag{3}$$

The packet dropping ratio is defined as the ratio of the total number of dropped packets ($N_{dr}$) over the packets that are received ($N_r$).

$$R_{dr} = N_{dr}/N_r. \tag{4}$$

The ratio of the number of delayed packets ($N_{dl}$) to the number of received packets ($N_r$) represents the packet delaying ratio ($R_{dl}$) as shown in the following equation.

$$R_{dr} = N_{dl}/N_r. \tag{5}$$

Substituting (4) and (5) in (3), the expected probability that the node behaves as a malicious node is estimated. The actual node's behavior slightly varies from the estimated probability of a node to act as a malicious one as it also includes the dropped packets due to mobility and collision. Each packet is added to the successful transmission count after overhearing the forwarded packet to the next-hop. The measured $1 - P_m$ value in Eq. (2) is considered as the direct trust value $T_d$. Though checking the packet transmission is an additional process, it enables an effective detection of dropping and delaying attacks in the network.

The proposed indirect trust metric assists the source with partial knowledge and deduces a reliable decision regarding the trustworthiness of the nodes in the positive progress set. The source node periodically broadcasts a reputation request ($R_{req}$) message to all nodes in the positive progress set except the node for which it calculates the trust and receives a reputation response ($R_{res}$) message from other neighbors. The source node broadcasts the $R_{req}$ to nodes in the Ps, thus, preventing broadcasting it to all its 1-hop neighbors. This process considerably controls the overheads. Let $S$ compute the indirect trust value of the node $D(T_{id(S,\ i)})$. Let '$i$' represent a common neighbor between nodes $S$ and $D$. The total number of common nodes be represented as $k$. The source node calculates an indirect trust value of the node using the following equation.

$$T_{id(S,A)} = \left(\frac{1}{|k|}\right)\left\{\sum_{i=1}^{k}\left(T_{d(S,i)} * T_{d(i,D)}\right)\right\}. \tag{6}$$

*Certainty factor*: The direct trust value is sufficient to reach a more reliable conclusion, which happens only after enough direct interactions. For the newly arrived nodes, it is insufficient to decide the direct trust value with limited interactions. Therefore, the indirect trust value is necessary for newly arrived nodes. The proposed work employs the certainty factor, and it represents the confidence level of the trust value. If the number of direct interactions increases, the direct trust value becomes more vital than the indirect trust value.

A certainty factor, $C_{(S,i\in PS)}$ is calculated by the number of messages exchanged between the source node and nodes in the positive progress set. The certainty of a trust from the node $i$ $P_S$ to user $S$ in a CPOR is defined as follows,

$$C_{(S,i\in PS)} = [n_{ex}]\{1 + c\}^{-1}. \tag{7}$$

In (7), $c$ is a fixed integer. It is a constant so that the value of the certainty factor varies every time based on the value

```
                    /* Fine Tuned Trust Evaluation*/
Find_Fine_Tuned_Trust_Value ( )
    {
        for (p=0; p <|P_S^T| ; p++)
        {
            if (Q_T (p)<1)
            {
                Measure S_T;
                F_Trust = W_QT * Q_FT+ W_ST * S_FT
                Q_FT = d (n, d)/d (s, d)* c_1 * c_2
                P_Fg = (1-P_m) - P_b
                P_Fg = P_g
                Measure S_FT &F_Trust;
            }
        Sort nodes in (P_s^T) based on F_Trust
        for (p=0; p <|P_S^T| ; p++)
            for (k=1; k <|P_S^T| ; k++)
            {
              if (F_Trust)_p = (F_Trust)_k
              {
                 If (Q_FT)_p < (Q_FT)_k
                 Select node p for data forwarding;
                 Else
                 Select node k for data forwarding
              }
            }
        }
    }

    Where,
        p = 0, 1,… N :N - Number of nodes in P_S^T
        W_QT and W_ST : Weights that are assigned to the QoS and Social trust
      factor and W_QT + W_ST = 1
```

**Figure 3.** Fine-tuned trust evaluation.

of the number of messages exchanged between the source node and nodes in the positive progress set. Finally, the source calculates the total fine-grained trust value ($C_{\text{Trust}}$) based on direct and indirect trust. The source node $S$ computes the coarse-grained trust value of the nodes in positive progress set using the values obtained from (2), (6) and (7). As the number of messages increases, the direct trust value becomes more trustworthy than the derivations from the reputation information.

$$S_{\text{T}} = \left(\left(C_{S,i\in\text{PS}}\right) * T_{\text{d}(S,i\in\text{PS})} + \left(1 - C_{(S,i\in\text{PS})}\right) * T_{\text{id}(S,i\in\text{PS})}\right). \tag{8}$$

Moreover, the coarse-grained trust value, ($C_{\text{Trust}}$) incorporating both $Q_{\text{T}}$ and $S_{\text{T}}$ is shown in the following equation.

$$C_{\text{Trust}} = W_{\text{QT}} * Q_{\text{T}} + W_{\text{ST}} * S_{\text{T}}. \tag{9}$$

The nodes in the positive progress set that has a coarse-grained trust value greater than a predefined threshold value $C_{\text{Th}}$ forms the trusted positive progress set $P_{\text{S}}^{\text{T}}$ as shown in figure 2 with respect to $S$. Where, $W_{\text{QT}}$ and $W_{\text{ST}}$: Weights that are assigned to the trust factor and distance factor and $W_{\text{TF}} + W_{\text{DF}} = 1$. However, this metric does not judge whether the misbehavior is likely a result of malicious activity or not. To select the appropriate data forwarding node, the proposed work fine tunes both the $Q_{\text{T}}$ and $S_{\text{T}}$ using several contextual information.

## 4.2 *Fine-grained trust evaluation*

The fine-grained trust evaluation fine tunes both $Q_{\text{T}}$ and $S_{\text{T}}$ using various contextual information such as location, energy level, and connectivity. The context can change dynamically, when the network is dynamic, for example, due to node mobility or traffic. The CPOR takes several types of context into account simultaneously. To efficiently deal with the traffic and network dimensions, and to support node mobility, the CPOR adopts a geographical opportunistic routing approach in which the routing is performed on a hop-by-hop basis relying on link quality, battery energy, and backup scenario. In battery sensitive applications, a fast drop in battery level indicates the imminent exhaustion of energy, thus the protocol needs to prevent the

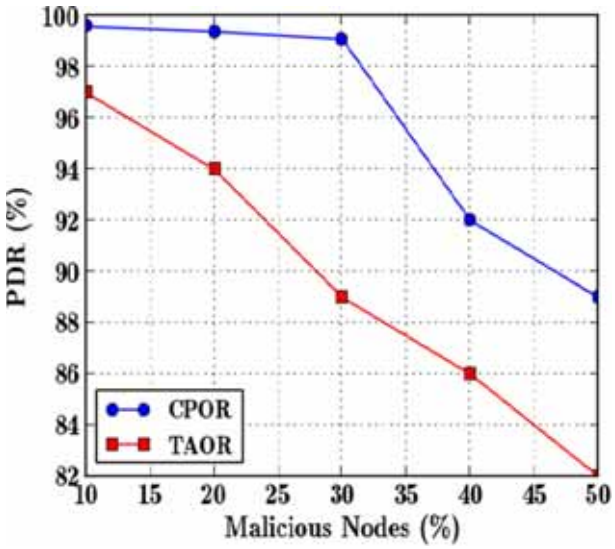


**Figure 4.** Malicious nodes vs packet delivery ratio.

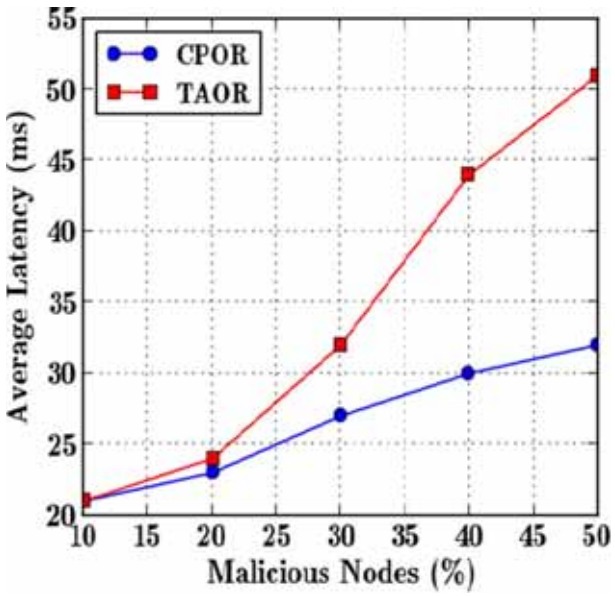


**Figure 5.** Malicious nodes vs average latency.

node from packet forwarding by reducing the weight of battery to save energy. Moreover, a good value of link quality indicates short progress, which reflects the less impact on node mobility, traffic, and interference on a link. The attacker and the activities of the backup nodes in opportunistic routing cannot be differentiated with the help of generic trust model alone. Thus, this work incorporates social contextual attribute such as a backup scenario in routing. These factors are used to determine whether the misbehavior is likely a result of malicious activity or due to network conditions. The context information of a node is defined as ($c_1$, $c_2$,…, $c_n$). The CPOR incorporates three types of context information: $c_1$ = link quality, $c_2$ = battery energy and $c_3$ = backup service to choose forwarders.

The CPOR enables network nodes to use information collected from the environment or users to participate in packet forwarding. The nodes in CPOR send a recommendation request to its entire 1-hop neighbors in the positive progress set and compute the trust value, in addition to the direct metrics. The source node sends a message requesting the beacon for context attribute ($c_{req}$) to the nodes in the positive progress set. The nodes in the trusted positive progressive set reply with their corresponding beacons of context attributes ($c_{rep}$). A node can obtain the contextual information by requesting the nodes in the trust positive progressive set through beacons. Moreover, each node attaches to the location of the destination in the ($c_{rep}$) packet, and the source node can estimate the distance of the nodes in the trusted positive progressive set.

4.2a *Fine-tune QoS trust*: An additive function is not a good choice for including all the context attributes in trust evaluation. Even if one attribute has a bad value, it makes the node undesirable. Because, this attributive, that have bad value may be compensated by other attributes. Thus, the CPOR exploits multiplicative in incorporating the contextual attributes such as $c_1$ to $c_2$ in fine tuning the QoS trust ($Q_{FT}$).

*Link quality and battery energy*: Each node in the communication range exchanges the hello packet periodically. The nodes are capable of measuring the link quality from its one-hop neighbors by exchanging hello packets on available channels in routing layer. The ratio of the number of successfully received hello packets ($R_r$) to generated packets (*T*/*I* where "*I*" represents the packet interval) is referred as link quality, $c_1$ is shown in Eq. (10). However, it is not possible to achieve high $c_1$ equal to *T*/*I*, because neighboring nodes not able to receive all the transmitted hello packets available on free channels. Moreover, the value of $c_2$ is measured in Eq. (11) using the remaining battery energy of a node in the positive progress sheet. Substituting (10) and (11) in (12), the expected probability that the node behaves as a reliable node is estimated.

$$c_1 = {(R_r * I)}/{T} \tag{10}$$

$$C_2 = 1 - (\text{User's requirement}/\text{Remaining battery energy}) \tag{11}$$

$$Q_{FT} = d(n,d)/d(s,d) * c_1 * c_2. \tag{12}$$

4.2b *Fine-tune social trust*: In an opportunistic routing, when a forwarding node does not forward the packet, the backup candidate transmits it towards the destination. According to the nature of opportunistic routing, the backup candidates do deny or drop the forwarding packets, when the main forwarding node transfer it. As a result, it may be misclassified as malicious node according to the

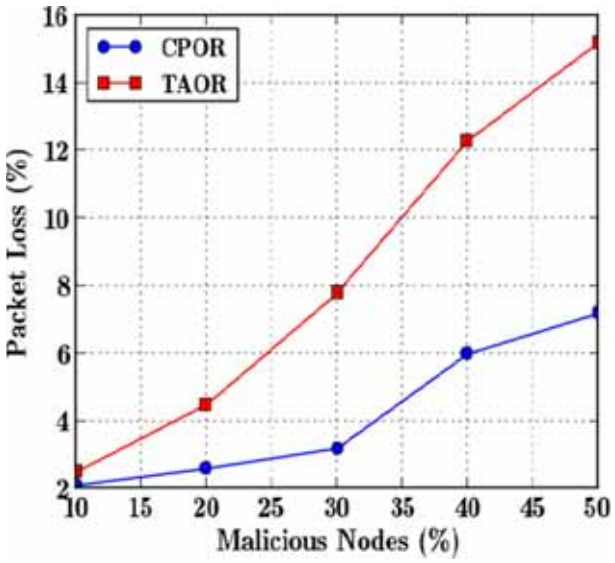


**Figure 6.** Malicious nodes vs packet loss.

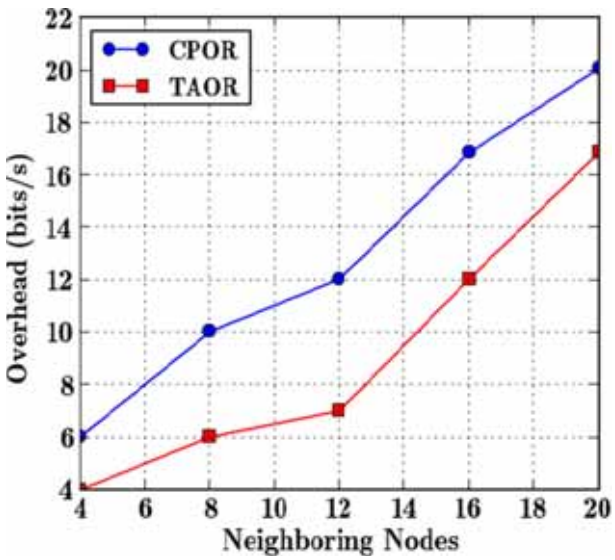


**Figure 7.** Neighboring nodes vs overhead.

rule of trust models. Thus, the standard trust formalization is not appropriate for an opportunistic routing.

*Backup service* ($c_3$): The probability of a node that well behaves is shown in Eq. (2). However, to improve the efficiency of trust value in an opportunistic routing, the probability that a node cooperates with the backup forwarding scenario is also included.

The trust metric considered in the backup forwarding scenario is the probability of successful backup service ($P_b$). It is not feasible to measure the cooperative service of a node when it acts as a backup node for others. Hence, CPOR enables only the nodes in the same that measures backup cooperative service for each other. Each node in $P_s$ measures and includes the backup node cooperative service in direct trust evaluation as shown in Eq. (2). While forwarding or higher priority nodes failing to transmit a packet, the backup node should forward the overheard packet, otherwise, it drops the data packet. Equation (2) is modified as

$$P_{Fg} = (1 - P_m) - P_b. \tag{13}$$

The $P_b$ is defined as the ratio of the summation of the number of successfully forwarded packets without duplication ($N_{fb}$). The number of successfully dropped packets ($N_{db}$) to the total number of packets received by a backup node is shown in the following equation.

$$P_b = \left\{ (N_{fb} + N_{db}) / N_{rb} \right\}. \tag{14}$$

The measured successful backup service value is considered in the estimation of the direct trust value of other nodes in the same positive progress set. However, these nodes appear as attackers in the view of others. Each node broadcasts the hello packets including successful backup service of its neighbors for every interval. The other nodes include the average trust value received from neighbors into its direct trust evaluation. Thus, the proposed work incorporates an efficient context sensitive social trust computation model ($S_{FT}$) and ensure the security.

$$S_{FT} = \left( \left( C_{(S,i \in PS)} * P_{Fg(S,i \in PS)} + \left(1 - C_{(S,i \in PS)}\right) * T_{id(S,i \in PS)} \right) \right) \tag{15}$$

$$F_{Trust} = W_{QT} * Q_{FT} + W_{ST} * S_{FT}. \tag{16}$$

By adjusting these weight factors, the importance of routing is switched between the QoS and Social trust-based routing. A brief description of the fine-tuned trust evaluation process is explained in figure 3. By using fine-tuned trust evaluation, the source node tunes the coarse-grained trust values of the nodes in a trusted positive progress set using context attributes like link quality, battery energy, and backup service. If two or more nodes have the same trust value of a fine-tuned trusted positive progress set relatively, the source node selects a data forwarding node that is closest to the destination among them.

### 4.3 *Null-trust zone*

The CPOR does not work in a situation; the source node does not find any trusted neighbor to forward the data packet towards the destination. The proposed CPOR finds this scenario as a communication "void" or "hole" zone and reaches the destination through an alternate path. This zone is called null-trust zone. The nodes that cannot find the trusted neighbors trigger the null-trust zone handling the process. To tackle with the null-trust zone, CPOR works

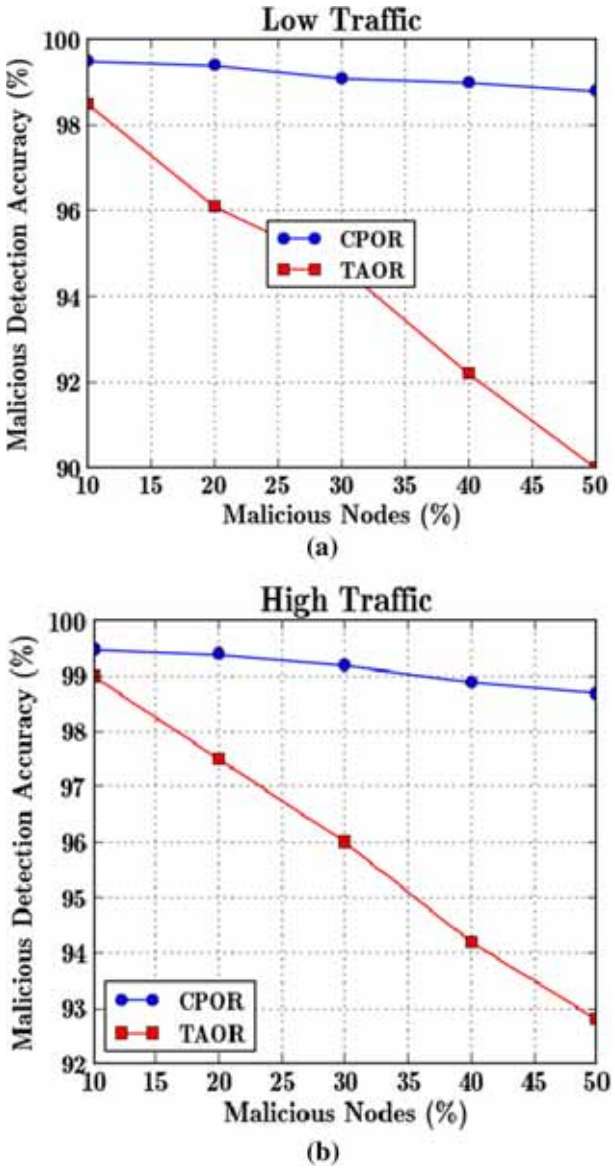


**Figure 8.** Malicious nodes vs malicious detection accuracy.

similar to the virtual destination based void handling (VDVH) mode in the POR [2]. CPOR finds a virtual temporary destination to which the packets are forwarded. The primary issue in handling this kind of void, when it is required to switch back to the standard greedy forwarding mode. Once a packet is forwarded to route around the communication void for more than two hops, the current node checks the packet for the potential node that is capable of switching back to the normal greedy mode. If the location of the temporary virtual destination node is nearer to the original destination, the mode switches to the standard greedy mode. In the case if the source node becomes the void node, it tackles the null-trust zone, and it triggers the process.

## 5. Analysis on CPOR

### Notations used

| | |
|---|---|
| C | Minimum achievable network capacity per hop |
| P | Probability to achieve $C$ in a link |
| $B_l$ | Bandwidth on link $l_{n,n1}$ |
| F | List of forwarding candidates |
| h | Next hop node |

### 5.1 *Impact on throughput of POR with malicious nodes*

In a highly dynamic network, the node mobility and data collision are the main reasons for the packet drop and throughput reduction. The opportunistic routing has been introduced to avoid the node mobility impact on network throughput. The achievable network capacity in the network without considering the node mobility and data collision is as follows.

$$C = \mathrm{MIN}\{B_i(n)\}. \tag{17}$$

From Eq. (17), it is indicated that the network capacity is equal to the link bandwidth that has a minimum bandwidth in the network. The probability of achieving $C$ in each link over a geographical routing is a function of node mobility and data collision. The probability that a node '$n$' delivers $C$ bits to the next hop node ($P_n$) over opportunistic routing within a second is shown in Eq. (18). Let $P_{ff}$ denote the failure of the forwarding candidate, and $P_{fb}$ denote the delay or the failure of the backup nodes' transmission to deliver $C$ bits/s.

$$P_n = 1 - (P_f * \Pi P_{bk}), \tag{18}$$

where $k \in F - h_n$.

Finally, the expected throughput i.e. number of bits delivered to the destination from the source node is denoted in Eq. (19). Where $(C_{generated})_s$ represents the generated bits per second at the source node. From Eq. (19), the average probability of packet delivery of the routing nodes decides the throughput, but it dynamically varies in geographical routing.

$$C_{expected} \approx \left(C_{generated}\right)_s * \mathrm{AVG}\left\{P_{(h_n)}\right\}, \tag{19}$$

where $n$ varies from 1 to $\{d(s - d)/R\}$.

However, the existence of malevolent nodes in the routing path degrade the network throughput, with the

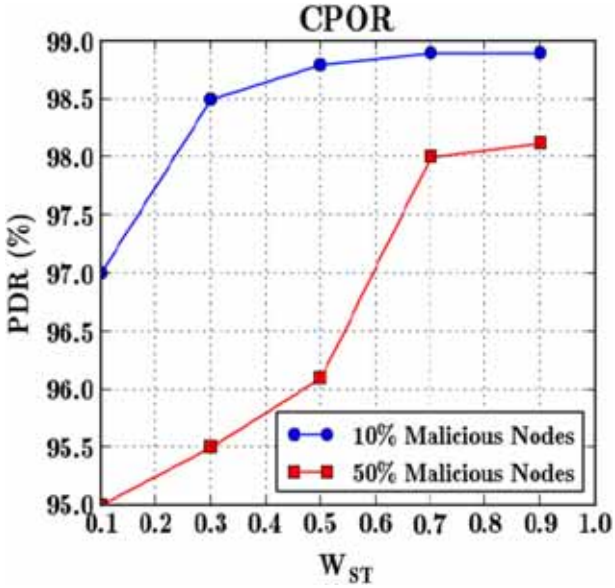


**Figure 9.** $W_{ST}$ vs packet delivery ratio.

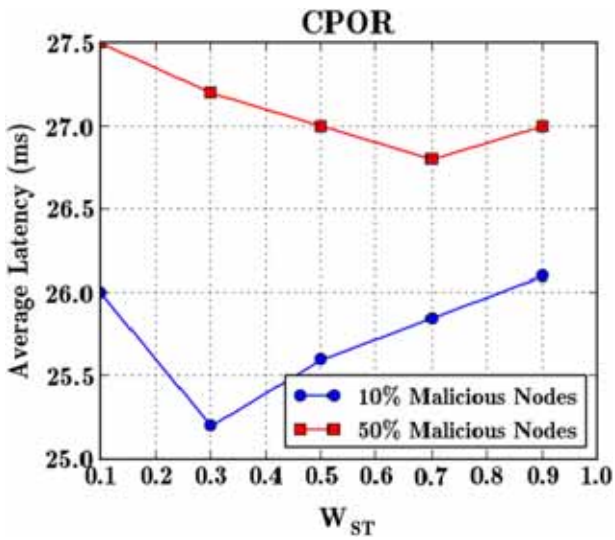


**Figure 10.** $W_{ST}$ vs average latency.

probability of a node '$n$' to deliver $C$ bits to a node ($h_n$) in the path.

### 5.2 *Throughput of CPOR with malicious nodes*

The proposed CPOR can isolate the malicious nodes successfully. However, it is hard to reach the expected through put as shown in Eq. (19), as it balances both the trust and the distance factors to select the optimal forwarding node effectively. It may lead to increase in the hop count to reach the destination, $h_{new} > h$.

$$C_{CPOR} = \left(1/|h_{new}|\right)\left\{\left(C_{generated}\right)_s * (P_m)_{h1} - \sum_{j=2}^{h_{new}} \left(C_{received}\right)_j * (P_m)_j\right\}. \quad (20)$$

### 5.3 *Overhead on CPOR*

The total number of packets used for routing and trust mechanism excluding the data packets is defined as the control overhead. Each node broadcasts the beacon packets for every interval (I) to exchange the location information with the neighboring nodes. The routing overhead of CPOR for a location exchange is shown in Eq. (22).

$$R_{overhead\ (location)} = (N * I). \quad (21)$$

It triggers another round of reputation messages to estimate the trust value of the neighbor nodes with $I_r$ interval. Therefore, it incurs higher overhead than the usual routing overhead in the POR. The routing overhead, including the reputation messages, is denoted as $R_{overhead\ (total)}$.

$$R_{overhead\ (total)} = (NI + 2NI_r). \quad (22)$$

## 6. Performance evaluation

This work uses the NS-2 simulator with CMU wireless extension to evaluate the performance of the proposed CPOR. This section describes the comparative simulation results of CPOR with an existing TAOR protocol [17]. The selection of the data forwarding node depends on both the fine-tuned QoS and the fine-tuned social trust metric. These factors help to select the trusted and optimal data forwarding node in CPOR. This work simulates the CPOR with a context-sensitive trust model in the area of 1000 × 1000 $m^2$ in which 100 nodes are randomly deployed with the moving velocity of 1–20 m/s. It simulates the IEEE 802.11 MAC layer with a node range of 75 m. The application and transport agents are the constant bit rate (CBR) and the user datagram protocol (UDP) respectively. A bandwidth of a node in the network is varied from 2 to 10 Mbps. CBR generates the data in an interval of 0.05 s with the size of 1024 bytes, and UDP configures the transport layer. The location update interval for nodes in the simulation is 1 s, and they take 10 s for trust management. The propagation model used is a TwoRayGround model. The network is simulated for 800 s.

### 6.1 *Impact of malicious nodes*

The performance of the proposed CPOR is analyzed by varying the number of malicious nodes from 10 to 50% in the network. Figure 4 shows the simulation results. The

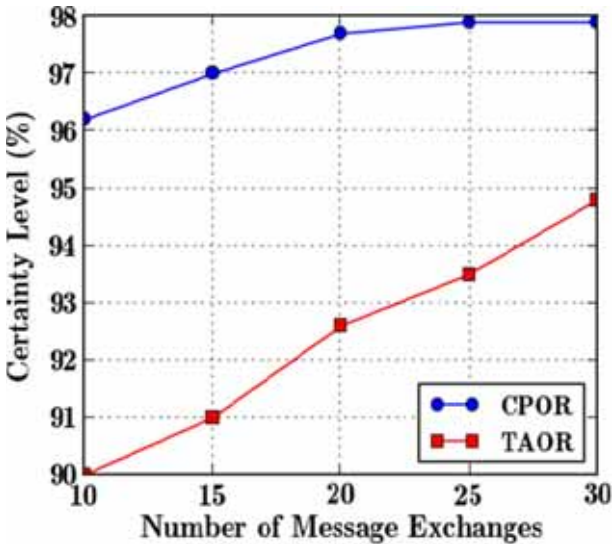


**Figure 11.** Number of message exchanges vs certainty level.

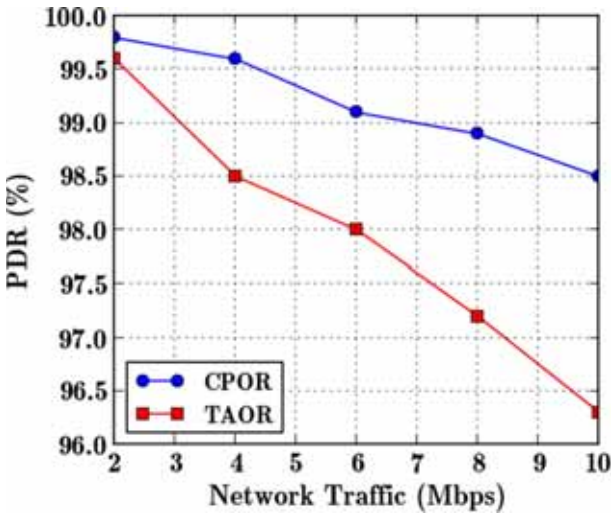


**Figure 12.** Network traffic vs packet delivery ratio.

consideration of QoS trust along with node's cooperative backup service of the trust model has lead to a higher packet delivery ratio in CPOR. Beyond the point of 30% of malicious nodes, the packet delivery ratio of both the trust models starts to degrade. An increase of more than 30% of the malicious nodes decreases the path availability to reach the destination by half. Beyond 30% of malicious nodes, the PDR gets reduced from 99% to 92% in CPOR, but it performs well in comparison with TAOR.

The proposed CPOR achieves better average latency compared to TAOR as the proposed work selects the most trusted nodes to route the packets towards the destination. TAOR quickly executes a trust evaluation and finds a trusted route when detecting malicious nodes. Thus, it behaves similar to the CPOR for a small fraction of malicious nodes. Besides, the proposed trust model achieves less communication latency, as it balances the QoS trust and the social trust. The CPOR considers the link quality, battery energy level and balances it with the direct trust. The forwarding node selection of CPOR leads to choosing the shortest, the long life path rather than the paths created by TAOR. From figure 5, it is observed, it shortens the path length in the network, this in turn reduces the packet latency to 37% from existing TAOR.

The packet loss represents the total number of data packets lost reasonably due to malicious node activities without any intimation. Figure 6 demonstrates the packet loss ratio for various percentages of malicious nodes. The CPOR finds the routing metric as the combination of the trust metric and the QoS metric (link quality, battery energy, and backup service) for optimal routing. However, the performance level of TAOR is far behind the proposed CPOR in terms of packet loss. In TAOR, the nodes cannot differentiate the malicious activities from the normal network conditions, and it leads to misclassification of the genuine node as malicious. The performance of the proposed work achieves optimal routing with a small packet loss when compared with TAOR. For example, Beyond 30% of malicious nodes, the packet loss gets increased from 3 to 7% in CPOR, but it performs well in comparison with TAOR by 53% at the point of 50% of malicious nodes.

The overhead of the proposed CPOR is high compared to the TAOR as shown in figure 7. If the number of neighboring nodes increases, the overhead of both the systems increases slightly. Though CPOR involves several processes for selection of the data forwarding node, the performance of CPOR is better in terms of PDR, as the proposed protocol balances the reliable and secure routing in terms of QoS and social trust. The TAOR applies one-hop hello packet flooding for location update and hence achieves less routing overhead, compared to CPOR. The overhead of CPOR increases the packet overhead by 15% than TAOR as shown in figure 7.

Detection accuracy represents the correctness of the trust model in detecting the malicious nodes. The detection accuracy of the proposed work is higher as it fine tunes the initially calculated trust values such as QoS and social trust as shown in figure 8. Since, the proposed work has calculated the accurate trust value; it differentiates the backup nodes from the malicious nodes and detects the malicious nodes with greater accuracy. The detection accuracy of the existing scheme reduces with the increase in the percentage of malicious nodes as shown in figure 8(a) and 8(b). For example, the TAOR achieves 97.5% of detection accuracy with high traffic, but it is decreased by 96% when the network traffic is low at the point of 20% of malicious nodes in the network. Because, it does not determine whether the misbehavior is likely a result of malicious activity or due to network conditions. Thus, when the false, malicious ratio of TAOR increases, the malicious detection

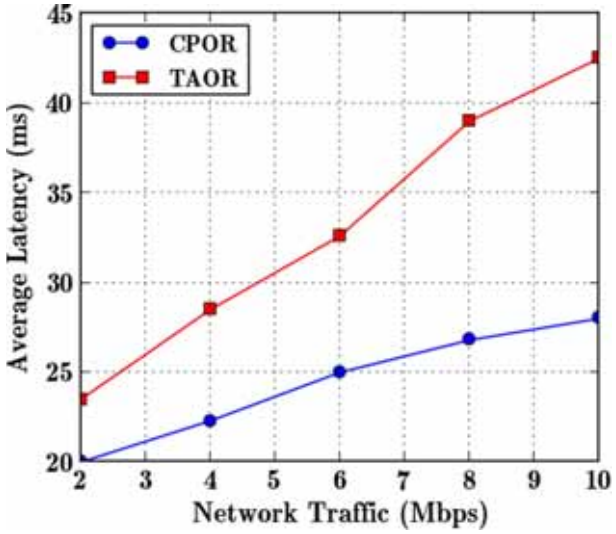


**Figure 13.** Network traffic vs average latency.

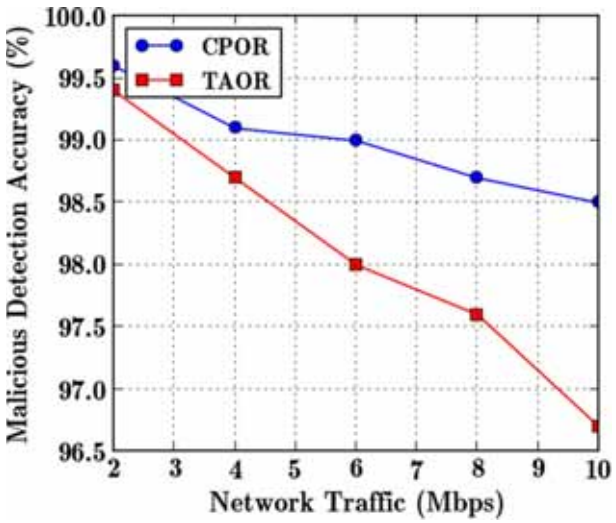


**Figure 14.** Network traffic vs malicious detection accuracy.

accuracy declines. The proposed CPOR is more confident about the trust value as it calculates the certainty factor based on the number of interactions among the nodes, and as well as the nodes' cooperative backup service.

### 6.2 *Impact of $W_{ST}$*

The performance of the proposed CPOR under the same network traffic is analyzed, by varying the $W_{ST}$ values from 0.1 to 0.9 with 10 and 50% of malicious nodes in the network. Figure 9 depicts the PDR of the proposed scheme for various values of $W_{ST}$. As estimated, the percentage of PDR is better when the $W_{ST}$ reaches sufficient point, and the PDR decreases with an increase in the percentage of malicious nodes. The PDR is superior with 3% of malicious nodes when it reaches $W_{ST} = 0.3$, but even with 50% of malicious nodes, it delivers superior PDF when it reaches $W_{ST} = 0.7$. There is no change in the performance, beyond $W_{ST} > 0.7$.

As the number of trusted nodes decrease, more weight is given only to the social trust factor and not to the QoS factor. The proposed system achieves optimal average latency at the point of sufficient $W_{ST}$. After reaching the common point of $W_{ST}$, the average latency increases as the packet has to travel long distance to reach the destination. For instance, the CPOR with 50% of malicious nodes takes 26.8 ms to deliver with the value of $W_{ST} = 0.7$ as shown in figure 10.

### 6.3 *Impact of number of direct interactions*

The certainty level is defined as the level of confidence in the trust value that a node has calculated with other nodes using the direct trust metrics. The TAOR is also confident about the trust value using the validation check. However, the proposed work tunes the trust value and also considers several contextual information such as link quality, battery status, and backup service. This is possible, to determine whether the misbehavior is likely a result of malicious activity or due to network conditions in CPOR. The certainty level of the proposed work is high when compared with the TAOR as shown in figure 11. The proposed work fine-tunes the trust value obtained from the QoS and the Social trust computation, thus obtaining the accurate trust value of a node. If the interactions are more than 20, the certainty level is closer to 98%.

### 6.4 *Impact of node's backup service*

The PDR and the average latency of CPOR are compared with CPOR and TAOR, by varying the network traffic from 2 to 10 Mbps as shown in figure 12 and figure 13. Each node acts as a forwarding candidate and also as a backup node. The CPORaccurately measure the behavior of the neighbor node, including the contextual information. In the case of high network traffic, the CPOR performs well as the consideration of link quality and battery energy in the finely tuned trust value reduces the packet loss due to node death. However, TAOR does not include the contextual attributes on evaluating the trust value. It marks honest nodes as misbehaving nodes, as the malicious behaviors due to the malicious activity and network conditions are equally treated as malicious without any further investigation. It reduces the PDR and increases the average latency of the TAOR by 33% more than that of CPOR.

Figure 14 illustrates the result of malicious detection accuracy of CPOR by varying the network traffic. In the face of high traffic scenario, the number of correct evidence

collected from the neighboring nodes is equal in both CPOR and TAOR, since only the nodes that act as sources measure the trust value for both the main and sub candidates in the TAOR. However, the proposed work enables all the nodes to measure the trust value of its neighboring nodes, including contextual information. Thus, it can calculate the accurate trust value of a node even in the low network traffic area; it detects the malicious nodes with greater accuracy. For example, the malicious detection accuracy of CPOR is reduced from 99.5 to 98.5%, when the network traffic is increased from 2 to 10 Mbps.

## 7. Conclusion

This paper has presented a context-aware trust model for secured geographic routing in MANET. The proposed trust model eliminates misbehaving nodes in the network with the context-sensitive trust model as it exploits several metrics for accurate trust evaluation. The coarse-grained trust value evaluates positive progress per hop and behavioral attributes that relate to the routing services. The proposed work relies on both the QoS and social trust metrics. Further, the coarse-grained trust value is fine-tuned based on contextual attributes. The CPOR selects the data forwarding node based on not only the trust factor, but also the contextual information such as link quality, the level of the battery energy, and backup service. It achieves the optimum balance between the reliability and the security and selects the most optimal and long-lived data forwarding node. The simulated results show the effectiveness of the CPOR, and it outperforms the TAOR. Unlike the existing systems, CPOR does not evaluate the trust on its entire one-hop neighbors, and thus it reduces the latency. It achieves a high PDR even in the presence of 50% of malicious nodes as compared to TAOR. The contextual attributes of CPOR enable to detect the malicious node with high detection accuracy compared to TAOR. When computing the trusted forwarding set, the trustworthiness value of the nodes is considered according to their current context. In the future work, to further improve the accuracy of social indirect trust value in CPOR, plans to enable the node to combine the evidences from different neighbors, only when it has a certain degree of belief of the neighboring nodes. This completely ignores the effect of conflict and improves the attack detection accuracy.

## References

[1] Shengbo Yang, Feng Zhong, Chai Kiat Yeo, Bu Sung Lee and Jeff Boleng 2009 Position based opportunistic routing for robust data delivery in MANETs. In: *Proceedings of IEEE Communications Society (GLOBECOM)*, pp. 1–6

[2] Shengbo Yang, Chai Kiat Yeo and Bu Sung Lee 2012 Toward reliable data delivery for highly dynamic mobile ad hoc networks. *IEEE Trans. Mobile Comput.* 11(1):111–124

[3] Tavakolifard M 2009 Situation-aware trust management. In: *ACM Proceedings of 3rd conference on Recommender Systems*, pp. 413–416

[4] Tavakolifard M, Herrmann P and Knapskog S J 2009 *Inferring trust based on similarity with TILLIT*. In: *Proceedings of 3rd International conference on Trust Management, IFIP Advances in Information and Communication Technology: Trust Management III*, Springer Boston, vol. 300, pp. 138–148

[5] Cahill V, Grey E, Seigneur J M, Jensen C and Chen Y 2003 Using trust for secure collaboration in uncertain environments. *IEEE Trans. Pervasive Comput. Mag.* 2

[6] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen 2011 A survey on trust management for mobile ad hoc networks. *IEEE Commun. Surv. Tutor.* 13(4): 562–583

[7] Ricardo Neisse, Maarten Wegdam, Marten van Sinderen and Gabriele Lenzini 2007 Trust management model and architecture for context-aware service platforms. In: *ACM Proceedings of the OTM Confederated International Conference on "On the move to meaningful internet systems: CoopIS, DOA, ODBASE, GADA and IS"*, vol. 2, pp. 1803–1820

[8] Melanie Hartmann, Holger Ziekow and Max Muhlhauser 2007 Context aware routing in sensor networks. *IEEE ITG-GI conference on Communication in Distributed Systems*, pp. 1–6

[9] Jiaxi You, Dominik Lieckfeldt, Frank Reichenbach and Dirk Timmermann 2009 Context-aware geographic routing for sensor networks with routing holes. *IEEE Conference on Wireless Communication and Networking*, pp. 1–6

[10] Mirco Musolesi and Cecilia Mascolo 2006 CAR: Context-aware adaptive routing for delay tolerant mobile networks. In: *ACM Proceedings of the International Conference on Wireless Communications and Mobile Computing*. pp. 533–538

[11] Maria Moloney and Stefan Weber 2005 A context-aware trust-based security system for ad hoc networks. *IEEE Workshop of the 1st international conference on Security and Privacy for Emerging Areas in Communication Networks*, pp. 153–160

[12] Paul K and Westhoff D 2002 Context aware detection of selfish nodes in DSR based ad-hoc networks. *IEEE Conf. Global Commun.* 1: 178–182

[13] Zahariadis T, Trakadas P, Leligou H C, Maniatis S, Karkazis P 2013 A novel trust-aware geographical routing scheme for wireless sensor networks. *Wirel. Personal Commun., Springer* 69(2): 805–826

[14] Leligou H C, Trakadas P, Maniatis S, Karkazis P and Zahariadis T 2012 Combining trust with location information for routing in wireless sensor networks. *Wirel. Commun. Mobile Comput.* 12(12): 1091–1103

[15] Joana Urbano, Ana Paula Rocha and Eugenio Oliveira 2010 Trust estimation using contextual fitness. In: *ACM Proceedings of the 4th KES International Conference on Agent and Multi-agent Systems: Technologies and Applications*, vol. 1, pp. 42–51

[16] Wenjia Li, Anupam Joshi and Tim Finin 2013 CAST: Context-aware security and trust framework for mobile ad-hoc networks using policies. *ACM Trans. Distrib. Parallel Databases* 31(2): 353–376

[17] Salehi Mahmood and Azzedine Boukerche 2014 Trust-aware opportunistic routing protocol for wireless networks. In: *Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, pp. 79–86