ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
DOI: 10.17559/TV-20150207070245

SUBJECTIVE LOGIC BASED TRUST MODEL FOR GEOGRAPHIC ROUTING IN MOBILE AD HOC NETWORKS

A. Rajesh, V. Raji, N. Mohan Kumar

Original scientific paper
In the past decades, several trust models have been proposed to enhance the security of Mobile Ad hoc Networks (MANETs). The conventional trust models fail to express the notion of uncertainty during the establishment of trust relationships between mobile nodes. Furthermore, they lack in considering the context attributes in trust evaluation. This paper proposes a subjective logic based trust model in POR (SLT-POR) that integrates both the behavioural and context based trust in trust model. The behavioural based trust incorporates subjective logic based evidence fusion in indirect trust evaluation to explicitly represent and manage ignorance as uncertainty. The trust relationship between nodes cannot always reflect the actual relationship and consequently the executed decision from the extracted trust relationship is not always accurate. The subjective logic theory includes a dynamic base rate operator that evaluates an expectation of an opinion and handles the uncertainty in evidence collection. In context, attributes based trust measurement, the SLT-POR estimates a context based trust value using the contextual attributes of each node in the trusted positive progress set. The SLT-POR considers the battery power to include node's lifetime in the trustworthiness estimation. It assigns a weight for both behaviour and context based trust to efficiently calculate total trustworthiness of a node. The simulation results demonstrate that the packet delivery ratio of the proposed SLT-POR is high even if 50 % of total nodes are malicious and outperforms Context-Aware Security and Trust (CAST) framework.

Keywords: *behavioural-based trust; contextual attributes; MANETs; POR; subjective logic; trust model*

Na logici zasnovan subjektivni model pouzdanosti za geografsko praćenje u pokretnim ad hoc mrežama

Izvorni znanstveni članak
Prošlih desetljeća predloženo je nekoliko modela pouzdanosti kao bi se povećala sigurnost mobilnih ad hoc mreža (Mobile Ad hoc Networks - MANETs). Uobičajeni modeli pouzdanosti ne uspijevaju izraziti pojam nesigurnosti tijekom uspostavljanja pouzdanih odnosa između pokretnih čvorova. Nadalje, nedostaje im uvažavanje značajki okoline u ocjeni pouzdanosti. U radu se predlaže model pouzdanosti zasnovan na subjektivnoj logici u POR (SLT-POR) koji u modelu integrira pouzdanost zasnovanu na kontekstu i onu zasnovanu na ponašanju. Pouzdanost zasnovana na ponašanju uključuje fuziju evidencije zasnovane na subjektivnoj logici u evaluaciji indirektne pouzdanosti kako bi se eksplicitno predstavilo i upravljalo neznanjem kao nesigurnošću. Odnos pouzdanosti između čvorova ne može uvijek odražavati stvarni odnos te stoga provedena odluka iz izvedenog odnosa pouzdanosti nije uvijek točna. Teorija subjektivne logike uključuje dinamičkog operatora osnovne brzine koji procjenjuje očekivanje mišljenja i bavi se nesigurnošću u skupljanju podataka. U mjerenju pouzdanost zasnovane na obilježjima konteksta, SLT-POR procjenjuje vrijednost pouzdanosti zasnovane na kontekstu uporabom kontekstualnih obilježja svakog čvora u nizu pozitivnog pouzdanog djelovanja. SLT-POR u procjeni pouzdanosti pazi da snaga baterije uključuje vijek trajanja čvora, pridaje važnost pouzdanosti zasnovanoj na kontekstu kao i onoj zasnovanoj na ponašanju kako bi učinkovito izračunao ukupnu pouzdanost čvora. Rezultati simulacije pokazuju da je omjer isporuke paketa predloženog SLT-POR visok, čak i ako je 50 % svih čvorova maliciozno te da je bolji od sustava CAST - Context-Aware Security and Trust.

Ključne riječi: *kontekstualna obilježja; MANETs; model pouzdanosti; POR; pouzdanost zasnovana na ponašanju; subjektivna logika*

1 Introduction

A mobile ad hoc network (MANET) is a collection of self-organized wireless mobile nodes. The nodes in MANET communicate with each other through single or multi-hop manner. Routing protocols are used to route the data packet from the source to the destination. Position based Opportunistic Routing (POR) is the latest geographic routing protocol based on the opportunistic forwarding in MANETs [1, 2]. Location awareness simplifies the routing in MANETs with increased privacy concerns. Due to the nature of the communication medium, the malicious nodes are likely to involve in malicious activities to disrupt the POR routing process. Evaluating the trustworthiness of the nodes in the router selection significantly improves the routing performance, as the trust model accurately reflects the actual behaviour of nodes.

A trust management scheme relies on two types of observations, namely as direct and indirect to evaluate the behaviours of nodes. In the direct trust, the nodes estimate trust for their neighbours by observing the communication behaviour. The standard routing exploits the indirect trust in which the trustworthiness of a node is collected as evidence from various observers. The indirect trust model escalates the trust prediction accuracy. Nevertheless, it fails to express the notion of ignorance during the establishment of trust relationships between mobile nodes. A highly trusted node is likely to fail in forwarding a packet due to the network conditions such as node energy, link quality, and the number of backup nodes. The context is a type of information that describes the entity's situation. The context specification has to be dynamic to accommodate the changes in the system and environment. The trust management strategy should be situation-specific to act accordingly [3, 4]. The concept of context is essential for developing trust-based security architecture, particularly for a network with a dynamic configuration such as MANET [5].

This work proposes a Subjective Logic based Trust model in POR (SLT-POR) to improve the routing performance. The SLT-POR initially calculates the trustworthiness of each node in the positive progress set based on the trust over behavioural and context attributes. The behavioural based trust value depends on both the direct and indirect trust metrics. To provide an appropriate direct trust computation for a node in an opportunistic routing, the SLT-POPR takes the node's cooperation for routing it as the proper trust evidence. It collects and combines the evidence from various observers using the subjective logic method in indirect trust estimation. In context attributes based trust, the SLT-

POR exploits some context attributes such as battery power, link quality, and the number of backup nodes.

1.1 Contributions

- The main contribution of SLT-POR is to design a behavioural and context attributes based trust model to ensure secure POR and also improve the routing efficiency.
- The SLT-POR involves in behavioural and context based trust evaluations. The behavioural trust includes the direct and indirect trust measurements, and the context trust value depends on contextual attributes.
- In behavioural trust measurement, the direct trust is calculated by overhearing the communication behaviour of nodes. The indirect trust is estimated by fusing the collected evidence from different observers based on the subjective logic method.
- The subjective logic method improves the decision accuracy of indirect trust estimation by including an effective base rate. The base rate operator estimates the expectation of opinion based on the number of positive evidence collected from observers and reduces the uncertainty.
- The consideration of contextual attributes, including the battery power, link quality and number of backup nodes in the context based trust evaluation drives the routing decision, allowing for shifting the emphasis from the selection of the most trusted path to reliable and long-lived one.

1.2 Paper organization

The structure of the paper is as follows. Section 2 discusses the related works of SLT-POR. Section 3 describes the system model of SLT-POR. Section 5 describes the forwarding region or positive progress set of a node in SLT-POR. The trust model of SLT-POR is explained in section 4. Section 5 evaluates the performance of SLT-POR. Section 6 concludes the paper.

2 Literature survey

A complete survey and various aspects of trust management on MANET are presented in [6]. The proposal in [7] identifies context-aware trust relationships that enable the users to select the most trustworthy services. The primary drawback 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 improve 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. The nodes in this network estimate the message importance locally using the knowledge base stored in them. A geographic routing algorithm with context awareness detects the holes if any, in the network [9]. This algorithm is known as HOle-Bypassing routing with Context-AwareNess (HobyCan). The routing algorithm sets up several alternative paths to bypass holes in the network. The Context-aware Adaptive Routing (CAR) protocol ensures delay-tolerant MANET routing [10]. The CAR exploits the prediction concept to route the message packets effectively and considers nodes as message carriers during the network separation to attain a better delivery rate. The CAR selects the best and suitable message carriers using prediction methods of the Kalman filter and utility theory.

A trust based decentralized security architecture confronts with the challenges of security management and context awareness computation in [11]. This security architecture establishes suitable trust levels for any context. This approach makes use of two projects, SECURE, and Aithe. SECURE uses the trust engine and 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 DSR [12]. It punishes the malicious and misbehaving nodes in the network. Though, the context-aware technique detecting the selfish nodes effectively, it uses a digital signature for disseminating information to intimate about the malicious nodes. An approach in [13] proposes a secure routing protocol that follows a distributed trust model and geographical routing strategy. The routing decision is taken based on the location, trust, and energy information. The proposal in [14] incorporates trust in geographic routing schemes such that it also balances the trust and location information.

The concept of context supports the trust management system [15]. It introduces Contextual Fitness, a component of the Computational Trust and Reputation (CTR) system that appends context information into the loop of trust management. The notion of Contextual Fitness empirically optimizes the trust values in a context-aware manner. The CAST protocol for MANETs exploits contextual information to detect the misbehaviour in the network [16]. An approach in [17] proposes a trust-aware secure routing framework (TSRF) that resists against several attacks in wireless sensor networks. It uses an adaptive exponential decay time factor to detect the attack and assigns the weight based on the context. The threshold value of the trust path is selected in the context of different applications. The work in [18] expands and enriches the subjective logic theory with a dynamic base rate operator and it promotes the extended subjective logic to the development of the trust theory. A novel subjective logic based trust model in [19] enables mobile nodes to represent explicitly and manage ignorance as uncertainty during the establishment of trust relationships with other nodes. The existing trust models do not consider the ignorance in evidence fusion. Also, lack of considering the appropriate context attributes in the trust evaluation accuracy of the estimated context-aware trust value degrades the detection accuracy. Some of the security mechanisms have to depend on using costly cryptography techniques which are not feasible in resource-limited MANETs.

3 System model

The autonomous network is considered as a graph G (N, E). The terms V and E represent the number of nodes and set of direct communication links between two nodes

respectively. Assume that each node accurately knows its position and the position of its neighbouring nodes. The range of node connectivity is limited to one-hop and bounded by the maximum distance R. The geographic location of each node in N is represented as $L(N) = (N_X, N_Y)$ where N_X and N_Y represent the coordinates. Consider a node $S \in N$ with the location (S_X, S_Y) and N_S is the one-hop neighbourhood of S. Let $D_{S\text{-}NS}$ be the distance between S and N_S. S selects its positive progress set to N_S, $P_S = \{1, 2, 3, \ldots, n\}$ considering the (S_X, S_Y) as a reference point. Each node traces its one hop neighbour's activities by overhearing. The direct trust metric, DT_n includes packet forwarding service on a node n. The indirect trust, IDT_n on node n is calculated using the subjective logic that includes the base rate (a) to manage uncertainty. The context based trust considers set of context attributes such as node energy (E), Link Quality (LQ), and the number of backup nodes (BN_n). Each node maintains a trusted repository to store the trust value on each metric for each of its one-hop neighbours.

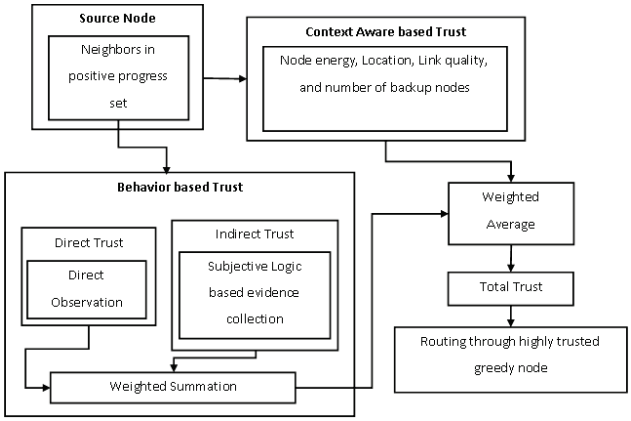

Figure 1 Block Diagram of SLT-POR Protocol

4 An overview of SLT-POR protocol

The proposed SLT-POR protocol extends the POR protocol with subjective logic based trust model. The SLT-POR takes the advantages of the stateless property of geographic routing. Initially, the source in SLT-POR forms positive progress set that contains greedy routers which are closer to the destination. With the aim of selecting a highly trusted greedy router, the source evaluates the trust of each greedy router in the positive progress set based on their behaviour and context attributes. Trust evaluation integrates both the direct and indirect trust metrics. A node estimates direct trust of its neighbour based on the one to one interaction. The SLT-POR evaluates the indirect trust using the subjective logic that enables mobile nodes to represent explicitly and manage ignorance as uncertainty during the establishment of trust relationships with other nodes. The SLT-POR takes weighted addition for both the direct and indirect trust and it evaluates a trust of a node. A highly trusted node is likely to drop the routing packets due to drained energy. To accurately deviate the malicious behaviour from normal, the SLT-POR takes into account the context attributes in trust evaluation. It evaluates total trust for a node by taking a weighted average of both direct and indirect trust values of the corresponding node. Moreover, the source forwards the routing packets to the destination through a highly trusted greedy node. The block diagram of SLT-POR is shown in Fig. 1.

4.1 Trust model

A trust is defined as the level of belief that a node puts on another node for a particular action according to communication behaviours. The trust value is utilized to identify whether a node is acting as a legitimate one or malicious. The trust model of SLT-POR includes two components, namely behavioural based trust and context aware based trust. The behavioural based trust considers both the direct and indirect trust in trust evaluation. The SLT-POR exploits subjective logic based evidence collection in indirect trust evaluation to effectively deal with uncertainty caused by noisy communication channels and high mobility nodes. The context aware based trust includes the context attributes such as node energy, location, link quality, and the number of backup nodes in evaluating the trust of a node. The trustworthiness of a node, T_n is estimated as follows.

$$T_n = \frac{W_1 \cdot BT_n + W_2 \cdot CT_n}{2}. \quad (1)$$

The behavioural and context trust of a node (n) is represented as BT_n and CT_n. The summation value of weighting factors W_1 and W_2 is equal to one.

4.1.1 Behavioural based trust

The behavioural based trust model integrates both the direct and indirect trust measurements. It measures the direct trust based on the routing activities. The indirect trust is measured based on subjective logic evidence fusion method. As the subjective logic explicitly takes the uncertainty and belief into account during the establishment of trust relationship between nodes, it is suitable to model the situations that include uncertainty. The behavioural based trust model takes weighted average for both the direct and the indirect trust values to define the trustworthiness of a node. The SLT-POR estimates the behavioural trust of a node n as follows.

$$BT_n = \alpha_1 \cdot DT_n + \alpha_2 \cdot IDT_n. \quad (2)$$

In Eq. (2), DT_n and IDT_n refer to the direct and indirect trust of a node n respectively. The terms α_1 and α_2 are weighting factors, where $\alpha_1 + \alpha_2 = 1$.

Direct trust measurement

The nodes in MANET communicate with neighbouring nodes to perform their tasks. The SLT-POR computes the direct trust based on the direct observation of routing interactions of one hop neighbours. The direct trust of node n, DT_n is estimated using the following equation.

$$DT_n = \frac{N_{\text{successful}}}{N}. \quad (3)$$

In Eq. (3), $N_{successful}$ and N refer to the number of successfully forwarded packets and the total number of packets. However, a node may fail to observe the behaviour of its neighbours continuously due to high mobility. Therefore, it is crucial to collect the indirect trust from neighbouring nodes in order to accurately estimate the trust of a node.

Subjective logic based indirect trust measurement

The SLT-POR computes indirect trust of a node n by fusing the recommended trust values that are collected from neighbouring nodes of node *n*. The SLT-POR exploits the advantage of subjective logic based trust model in combining the evidence that is collected from various observers. The subjective logic enables mobile nodes to explicitly represent and manage ignorance as uncertainty during the establishment of trust relationships with other nodes. The subjective logic models the situations more realistically and it provides conclusions that more correctly reflect the uncertainty using the evidences that are collected from different observers. The subjective logic exploits a dynamic base rate operator (*a*) to estimate the expectation of an opinion. The base rate is an important parameter of subjective logic, as the expected level of opinion overcomes the uncertainty when the collected evidence is distinctive.

It is assumed that the dynamic base rate is equal to one for all nodes at the time of network initialization. After that, it varies between 0 ÷ 1 according to the number of positive evidence. Consider a source node establishes a trust for node n ϵ positive progress set. It collects evidence from node m and node p that are neighbours of node n. The nodes p and m provide evidence in the form of an opinion (ω_n^p) and (ω_n^m) as shown in Eq. (4) and (5) respectively. The subjective opinion (ω) has three dimensions such as belief (*b*), disbelief (*d*), and uncertainty (*u*). The terms belief and disbelief are epitomized from the evidence captured for legitimate and malicious behaviours respectively. Uncertainty represents the ignorance or level of confidence in a node's knowledge.

$$\omega_n^p = \left(b_n^p, d_n^p, u_n^p\right), \tag{4}$$

$$\omega_n^m = \left(b_n^m, d_n^m, u_n^m\right). \tag{5}$$

Eq. (4) presents an opinion (ω_n^p) in which belief (b_n^p) provides the trust value of probability of node p on node n depending on the benign behaviour of node n. Similarly, disbelief (d_n^p) represents the distrust value of probability of *p* on *n* depending on the malicious behaviour of node *n*. Moreover, uncertainty (u_n^p) represents the ignorance of probability of *p* on node *n*. If the collected evidence is observed in a different time interval, the SLT-POR combines the evidence as shown in Eq. (6).

When $U_p^m \neq 0 \vee u_n^p \neq 0$

$$\omega_n^{m\Diamond p} = \begin{cases} b_n^{m\Diamond p} = \dfrac{b_n^m u_n^p + b_n^p u_n^m}{\left(u_n^m + u_n^p - u_n^m u_n^p\right)} \\ u_n^{m\Diamond p} = \dfrac{u_n^m u_n^p}{\left(u_n^m + u_n^p - u_n^m u_n^p\right)} \end{cases}. \tag{6}$$

When $U_p^m = 0 \wedge u_n^p = 0,$ the SLT-POR combines the evidence using Eq. (7).

$$\omega_n^{m\Diamond p} = \begin{cases} b_n^{m\Diamond p} = \delta b_n^m + (1-\delta) b_n^p \\ u_n^{m\Diamond p} = 0 \end{cases}, \tag{7}$$

where,

$$\delta = \lim_{\substack{u_n^m \to 0 \\ u_n^p \to 0}} \left(\frac{u_n^p}{u_n^m u_n^p} \right). \tag{8}$$

In indirect trust evaluation, there are no direct communication behaviours between the source and the next forwarder. The source takes into account the evidence collected from the neighbouring nodes of a greedy node for trust calculation.

If the two nodes observe the behaviour of a neighbouring node in the same time interval, the SLT-POR combines the evidence using Eq. (9).

When $U_p^m \neq 0 \wedge u_n^p \neq 0$

$$\omega_n^{m\Diamond p} = \begin{cases} b_n^{m\Diamond p} = \dfrac{b_n^m u_n^p + b_n^p u_n^m}{\left(u_n^m + u_n^p\right)} \\ u_n^{m\Diamond p} = \dfrac{2u_n^m u_n^p}{\left(u_n^m + u_n^p\right)} \end{cases}. \tag{9}$$

When $U_p^m = 0 \wedge u_n^p = 0,$

$$\omega_n^{m\Diamond p} = \begin{cases} b_n^{m\Diamond p} = \delta b_n^m + (1-\delta) b_n^p \\ u_n^{m\Diamond p} = 0 \end{cases}, \tag{10}$$

where,

$$\delta = \lim_{\substack{u_n^m \to 0 \\ u_n^p \to 0}} \left(\frac{u_n^p}{u_n^m u_n^p} \right). \tag{11}$$

Moreover, the source combines the evidence using subjective logic theory and computes the indirect trust value of node *n*. By substituting the DT_n and IDT_n value in Eq. (2), the source evaluates overall trust of a node n.

Renovation of base rate

There are *N* observations in each interval, *r* and *s* which represent the number of the number of positive and negative evidence in the i^{th} period respectively. The base rate (*a*) is changed dynamically in each interval. For instance, if $r_1 = r_2$, the positive number of evidence in first and second period is equal, as a result, no changes occur in the base rate. If $r_1 < r_2$, the number of positive evidence in the second period is more than the first period, the base

rate has to increase. Similarly, $r_1 > r_2$, the number of positive evidence in the second period is lower than the first period, the base rate has to decrease.

4.1.2 Context aware based trust

The SLT-POR measures the trustworthiness of each node by taking into account both the direct and indirect trust value. A node that has high trust value may drop the packets due to drained energy or lower link quality or having no backup nodes. It is crucial to consider a set of context attributes in evaluating the trustworthiness of a node to improve the routing performance. The context attributes set (C_{Att}) is given in Eq. (12).

$$C_{\text{Att}} = \{E, LQ, BN_n\}. \tag{12}$$

The SLT-POR obtains the E and BN_n values using beacons. The source disseminates context attributes request, C_{req} in its area. The nodes in the positive progress set attach their E and BN_n values in context attributes reply (C_{rep}) and forward the C_{rep} to the source. Further, the source estimates link quality using the signal strength measurement. LQ is the ratio of signal power to the noise power, and it is estimated as follows.

$$LQ = \frac{(P_{\text{t}} / D)}{N_{\text{r}}}. \tag{13}$$

In Eq. (13), P_{t}, D, N_{r} represents the beacon transmitting power, the distance between the beacon transmitting and receiving the vehicle, and noise power respectively. The SLT-POR evaluates the Context trust of node n (CT_n) based on the C_{Att}.

Moreover, substituting the BT_n and CT_{n} values in Eq. (1), the SLT-POR estimates the T_n of a node n. Likewise, the source estimates trust for all nodes in the positive progress set and selects the most trustworthy node as a router.

5 Performance evaluation

The performance of SLT-POR is evaluated using Network Simulator-2 (NS-2). The SLT-POR is compared with an existing Context-Aware Security and Trust (CAST) framework [16]. The simulation is performed on a random topology of 100 nodes over a network area of 1000 × 1000 m. The moving velocity of nodes is 20 m/s. It simulates the IEEE 802.11 MAC layer with a node range of 75 m. The application and transport agents are CBR and UDP respectively. In NS2 simulation, Constant Bit Rate (CBR), and User Datagram Protocol (UDP) develops the communication model. CBR generates the data in a fixed interval in the network, and UDP configures the transport layer. The propagation model used is a TwoRayGround model. The network is simulated for 300 seconds.

5.1 Experimental results

The performance of the proposed SLT-POR is evaluated in different scenarios. The efficacy of the SLT-POR protocol is examined using performance metrics such as packet delivery ratio, average latency, and detection accuracy.

Packet Delivery Ratio (*PDR*): It is the ratio between the number of delivered data packets to the destination and the total number of generated packets.

Detection Accuracy: It is the percentage of successfully detected attackers in the network.

Overhead: It is the ratio of the number of additional packets used in the network to the total number of generated data packets.

Average Latency: The average time taken by a packet to travel from source to destination.

5.1.1 Impact of malicious nodes

Fig. 2 shows the result of the *PDR* of SLT-POR and CAST protocols, by varying the malicious nodes. Both the protocols decrease the *PDR* when increasing the malicious nodes from low to high. The reason behind this is that the high malicious scenario contains a huge number of malicious nodes in which the nodes do not cooperate in packet forwarding. For instance, the SLT-POR decreases the *PDR* by 2,15 %, when the malicious nodes vary from 5 % to 40 %. However, the SLT-POR outperforms CAST, as it exploits the advantage of subjective logic that accurately identifies the attacker. The CAST exploits Dempster-Shafer theory for evidence fusion that does not handle the ignorance under the high malicious scenario. In Fig. 2, the SLT-POR and CAST attain *PDR* of 96,65 % and 95,7 % respectively, when the network is 40 % malicious.

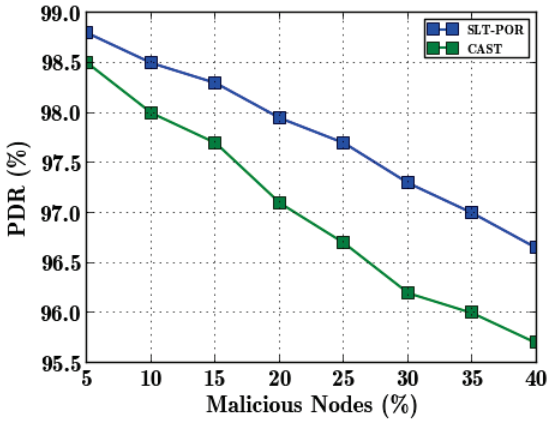

Figure 2 Malicious Nodes Vs PDR

The results of detection accuracy of SLT-POR and CAST are shown in Fig. 3. The detection accuracy of both protocols declines with the increase in the percentage of malicious nodes. However, the detection accuracy of SLT-POR is higher than CAST, as it accurately evaluates the trustworthiness of a node by exploiting subjective logic evidence fusion. Since the base rate provides an expectation of opinion that differentiates the normal nodes from the malicious nodes, it detects the malicious nodes with greater accuracy. With increased network traffic, the nodes increase the packet loss and delay. Thus, the false malicious ratio of CAST increases and the malicious detection accuracy gets reduced. For instance, the SLT-POR and CAST achieve detection accuracy of

97,05 % and 95,8 % respectively when the percentage of malicious nodes is 40.

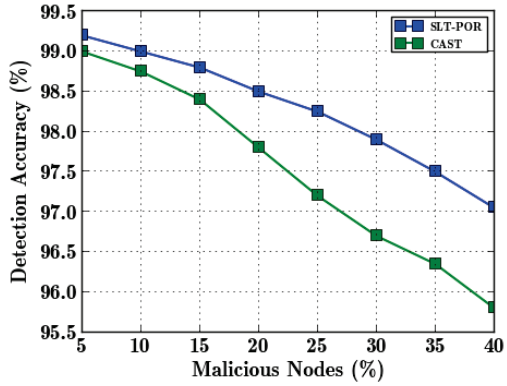

Figure 3 Malicious Nodes Vs Detection Accuracy

5.1.2 Impact of network traffic

Fig. 4 demonstrates that the PDR results in SLT-POR and CAST routing protocol. The results are obtained by varying the number of flows. Both the protocols decline the *PDR* when increasing the number of flows from low to high. The reason is that each node in POR is being responsible for acting as a forwarding candidate and also a backup node. The nodes are likely to drop packets due to network condition such as collision and drained energy. The proposed SLT-POR measures the context trust of a node based on context attributes such as battery power, Link Quality, and the number of backup nodes. As a result, the trust value of each node is measured accurately. In the case of high network traffic, the SLT-POR works well as the consideration of context attributes in trust evaluation reduces the packet loss. For instance, the SLT-POR increases the PDR by 1,12 % more than that of CAST under high network traffic scenario.

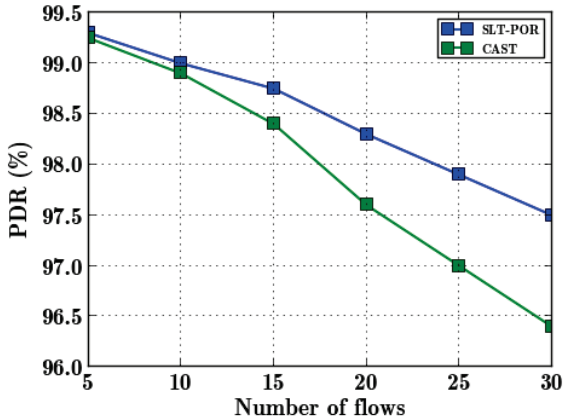

Figure 4 Number of Flows vs PDR

Fig. 5 illustrates the comparative results of detection accuracy of SLT-POR and CAST routing protocols by varying the number of flows in the network. The detection accuracy of SLT-POR and CAST decreases with increasing number of network flows. According to the network traffic, the opportunistic routing protocols exploit several nodes for backup service. In high network traffic scenario, the nodes in positive progress are marked as malicious, as these nodes are frequently exploited for backup, and they exhibit a large amount of energy for routing. The SLT-POR calculates accurate trust value of a node by considering the context attributes in trust evaluation, and it detects the malicious nodes with greater accuracy. As a result, the SLT-POR slightly decreases the detection accuracy with increasing number of flows. From Fig. 5, the SLT-POR increases the detection accuracy by 1,2 % higher than CAST when the number of flows is 30.

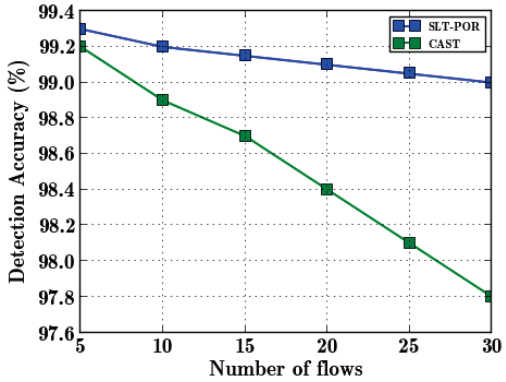

Figure 5 Number of Flows Vs Detection Accuracy

5.1.3 Impact of Number of Nodes

Fig. 6 shows the results of the overhead of SLT-POR and CAST protocols by varying the number of nodes. If the number of nodes is increased, the overhead of both the protocols increases slightly. Although, SLT-POR involves several processes for selection of data forwarding node, the overhead of SLT-POR is acceptable, as the trust is evaluated to a certain set of nodes. The CAST also collects evidence for trust evaluation, and hence, it achieves better performance. The SLT-POR and CAST attain an overhead of 21 % and 21,5 % respectively for 100 nodes.

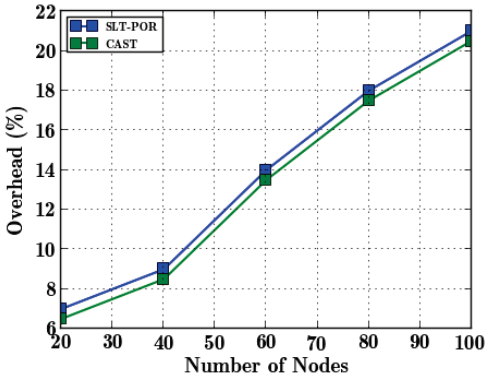

Figure 6 The Number of Nodes vs Overhead

From the comparative results that are illustrated in Fig. 7, both the SLT-POR and CAST protocols decrease the average latency, when increasing the number of nodes. The presence of a huge number of nodes in the network increases the connectivity, and the packets are delivered quickly at the destination. For instance, the SLT-POR attains an average latency of 0,3 seconds and 0,03 seconds in the presence of 20 and 100 nodes respectively. The SLT-POR achieves minimum average latency compared to CAST as it evaluates the trustworthiness of a node accurately by including a base rate operator. Further, it selects the most trusted nodes to

route the packets towards the destination. From Fig. 7 it is shown that the SLT-POR reduces the average latency by 27,85 % less than that of CAST for 20 nodes.

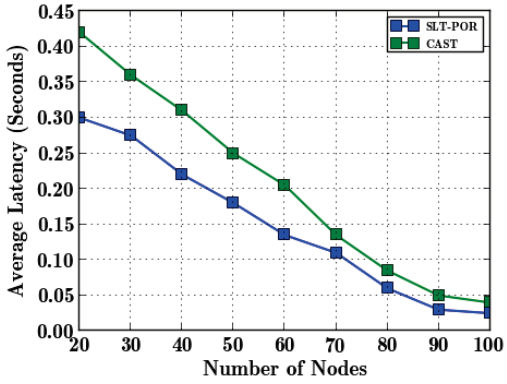

Figure 7 The Number of Nodes vs Average Latency

6 Conclusion

By integrating both the behavioural and context attributes in trust evaluation, the proposed SLT-POR significantly improves the security in POR. In behavioural trust measurement, the SLT-POR considers both the direct and indirect trust metrics. It collects and combines the evidence based on the subjective logic in which the base rate evaluates the expectation of the opinion that assists to deviate the normal and malicious behaviours accurately. The context aware trust calculates the trust using context attributes, and it reduces the packet loss due to node death. Moreover, the trust model of SLT-POR significantly improves the routing efficiency and detection accuracy. The simulation results show that the SLT-POR attains high *PDR* and detection accuracy when compared to the existing CAST protocol.

7 References

[1] Yang, Shengbo; Zhong, Feng; Kiat Yeo, Chai; Sung Lee, Bu; Boleng, Jeff. Position based Opportunistic Routing for Robust Data Delivery in MANETs. // Proceedings of IEEE Communications Society (GLOBECOM), 2009, pp. 1- 6.

[2] Yang, Shengbo; Kiat Yeo, Chai; Sung Lee, Bu. Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks. // IEEE Transactions on Mobile Computing. 11, 1(2012).

[3] Tavakolifard, M. Situation-aware Trust Management. // ACM Proceedings of the 3rd Conference on Recommender Systems. 2009, pp. 413-416.

[4] Tavakolifard, M.; Herrmann, P.; Knapskog, S. J. Inferring Trust based on Similarity with TILLIT. // Proceedings of 3rd International Conference on Trust Management, IFIP Advances in Information and Communication Technology: Trust Management III, Springer Boston, Vol. 300, 2009, pp. 138-148. DOI: 10.1007/978-3-642-02056-8_9

[5] Cahill, V.; Grey, E.; Seigneur, J. M.; Jensen, C.; Chen, Y. Using Trust for Secure Collaboration in Uncertain Environments. // IEEE transaction on Pervasive Computing Magazine, Vol. 2, 2003.

[6] Cho, Jin-Hee; Swami, Ananthram; Chen, Ing-Ray; A Survey on Trust Management for Mobile Ad Hoc Networks. // IEEE Communications Surveys & Tutorials. 13, 4(2011), pp. 562-583. DOI: 10.1109/SURV.2011.092110.00088

[7] Neisse, R.; Wegdam, M.; van Sinderen, M.; Lenzini, G.. Trust Management Model and Architecture for Context-Aware Service Platforms. // ACM Proceedings of the OTM confederated international conference on "On the move to meaningful internet systems: CoopIS, DOA, ODBASE, GADA and IS". 2, (2007), pp. 1803-1820.

[8] Hartmann, M.; Ziekow, H.; Muhlhauser, M. Context Aware Routing in Sensor Networks. // IEEE ITG- GI Conference on Communication in Distributed Systems. (2007), pp. 1- 6.

[9] You, J.; Lieckfeldt, D.; Reichenbach, F.; Timmermann, D. Context-aware Geographic Routing for Sensor Networks with Routing Holes. // IEEE Conference on Wireless Communication and Networking. (2009), pp. 1-6. DOI: 10.1109/wcnc.2009.4917638

[10] Musolesi, M.; Mascolo, C. CAR: Context-aware Adaptive Routing for Delay Tolerant Mobile Networks. // ACM Proceedings of the International Conference on Wireless Communications and Mobile Computing. (2006), pp. 533-538.

[11] Moloney, M.; Weber, S. 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. (2005), pp. 153-160.

[12] Paul, K.; Westhoff, D. Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks. // IEEE Conference on Global Communications. 1, (2002), pp. 178-182.

[13] Zahariadis, T.; Trakadas, P.; Leligou, H. C.; Maniatis, S.; Karkazis, P. A novel trust-aware geographical routing scheme for wireless sensor networks. // Wireless Personal Communications. 69, 2(2013), pp. 805-826. DOI: 10.1007/s11277-012-0613-7

[14] Leligou, H. C.; Trakadas, P.; Maniatis, S.; Karkazis, P.; Zahariadis, T. Combining trust with location information for routing in wireless sensor networks. // ACM Transaction on Wireless Communications and Mobile Computing. 12, 12(2012), pp. 1091-1103. DOI: 10.1002/wcm.1038

[15] Urbano, J.; Rocha, A. P.; Oliveira, E. Trust Estimation Using Contextual Fitness. // ACM Proceedings of the 4th KES international conference on agent and multi-agent systems: technologies and applications. 1, (2010), pp. 42-51.

[16] Li, W.; Joshi, A.; Finin, T. CAST: Context-Aware Security and Trust Framework for Mobile Ad-hoc Networks Using Policies. // ACM transaction on distributed and parallel databases. 31, 2(2013), pp. 353-376.

[17] Duan, Junqi; Yang, Dong; Zhu, Haoqing; Zhang, Sidong; Zhao, Jing. TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks. // International Journal of Distributed Sensor Networks. 2014, (2014), pp. 14. DOI: 10.1155/2014/209436

[18] Qiang, Jiao-Hong; Xin, Wang-Xin; Feng, Tian-Jun. Improved Dynamic Subjective Logic Model with Evidence Driven. // Journal of Information Processing Systems. 11, 4(2015), pp. 630-642.

[19] Balakrishnan, Venkat; Varadharajan, Vijay; Tupakula, Uday. Subjective Logic Based Trust Model for Mobile Ad hoc Networks. // Proceedings of the 4th International conference on Security and privacy in communication networks. 2008. DOI: 10.1145/1460877.1460916

Authors' addresses

A. Rajesh, Assoc. Professor
S. K. P. Engineering College,
Department of Computer Science and Engineering,
Thiruvannamalai – 606 611, Tamil Nadu, India
E-mail: sishnuraj7@yahoo.co.in

V. Raji, Asst. Professor
S. K. P. Engineering College,
Department of Computer Science and Engineering,
Thiruvannamalai – 606 611, Tamil Nadu, India
E-mail: raji.vpm@gmail.com

N. Mohan Kumar, Professor
S. K. P. Engineering College,
Department of ECE,
Thiruvannamalai – 606 611, Tamil Nadu, India
E-mail: nmkphdju@gmail.com