# cTrust: COMPLEMENTARY TRUST BASED ROUTING IN MULTI-HOP WIRELESS MESH NETWORKS

**P. Subhash[1], S. Ramachandram[2]**

**[1] Department of CSE, JITS, A.P, India**
**[2] Department of CSE, UCE, Osmania University, A.P, India**

***ABSTRACT:*** Routing in wireless mesh network has focused on the airtime link metrics to maximize throughput. On the other hand the assumption, "all the nodes are honest and cooperate correctly", to compute metrics and forward data causes unpredictable disruption of the network if a node gets compromised. A number of protocols have been proposed to address this issue by employing trust and reputation in routing decisions. These protocols either directly employ trust or integrate trust with the existing routing metric in making routing decisions. The former technique clearly does not suit a network whose throughput requirements are high and the latter does not always achieve optimal performance. In this paper, we show that integrating trust with the employed routing metric does not always yield optimal performance. Further, we propose a complementary trust based routing mechanism that complements the existing routing metric instead of integrating trust. The performance of our model is analyzed and compared with the existing models that integrate trust with the underlying routing metric. The results show the improvement in performance by employing our approach and are better than the earlier protocols.

***KEYWORDS:*** Wireless Mesh Network, Routing Metric, Trust.

## I. INTRODUCTION

Wireless Mesh Networks (WMNs) are multi-hop wireless networks with self-healing, and self configuring capabilities. These features, when combined with the ability to provide wireless broadband access, reduce the deployment cost and administrative overhead considerably. The main application of WMN technology is to provide wireless connectivity inside a building, campus, on a large geographical area or at a disaster site without requiring every access point to be physically connected to the Internet [AWW05]. These unique features of WMNs have generated considerable interest in the industry and academic fields.

However, there are still many issues that need to be addressed. Design of an optimal routing protocol is one such issue that needs to be addressed. As WMNs are expected to support high throughput internet applications, the routing metric and routing protocol employed determines the amount of throughput achieved. Several different routing protocols have been proposed that exploit the unique features offered by WMNs [C+03, KB06, DPZ04, Cou04, YWK05]. These protocols are similar in a way that they discover routes either in a reactive or in a proactive fashion. On the other hand, the major difference between these protocols is the kind of routing metric employed. Routing metrics employed by these protocols are designed to exploit different characteristics of a wireless link. The major characteristics that need to be considered are high variability in wireless links; varying available bandwidth and intra (and inter) flow interference [SBM06]. The main motive of these routing metrics is to address the link characteristics in a way to increase the overall throughput. Apart from these link properties the other important characteristic that needs to be considered is the selfish and malicious behavior of the WMRs.

The nodes (WMRs) in the wireless mesh backbone work collaboratively to discover and route the client traffic around the network. Due to the distributed network architecture of a WMN and shared wireless medium, the nodes can be easily compromised by an adversary. Moreover, in a community based WMN where nodes are managed by different operators, WMRs tend to exhibit selfish behaviour by forwarding its own traffic. The main aim of malicious nodes is to disrupt smooth functioning of the network. The majority of research that has been carried out to address this problem employs trust to carry out network activities [AH98, GPM04, DVU06, YZV03, OR08, P+11]. Employing trust solely in the route-selection process allows the nodes to establish a path through trustworthy nodes, but fail to achieve high throughput as they ignore wireless link properties. Integrating trust value of a node/link with the existing routing metric is an alternate way of discovering routes [P+11]. But, even this integration process does not achieve good results as we will prove that these two entities (routing metric and trust) are independent and if integrated fail to achieve optimal performance.

In this paper, initially we show how integrating the trust with routing metric does not yield optimal performance and later present a trust model that complements the existing routing metric. We will also show the analysis of our approach that achieves better performance over metrics that integrated trust and

routing metric. The rest of the paper is organized as follows. Section II presents the related work and problems with existing approaches. The orthogonality of trust and routing metric is provided in Section III. We present our complementary trust based routing approach in section IV. The simulation results are shown in section V along with the analysis of the results. Finally, section VI concludes the paper.

## II. RELATED WORK

Recently, a lot of research has been carried out to increase the performance of routing protocols in WMNs. The main design goal of these routing protocols is throughput maximization, even at the expense of generating more routing overhead, that deserves a secondary role [KHP08]. Therefore, a majority of the research that has been carried out focuses on the design of routing metrics that increase the overall throughput offered by the network. Metrics such as ATLM (airtime link metric) [Bah07], ETX (expected transmission count) [C+03], ETT (expected transmission time), WCETT (weighted cumulative ETT) [DPZ04] and mETX (modified ETX) [KB06] have been developed replacing hop-count. Their main design aim is enhanced performance and increased throughput. These metrics are modeled by assuming the co-operation among participating nodes. This assumption does not hold for any distributed network that operates in an open wireless medium including WMN, where the nodes can be easily compromised by an adversary. Therefore, further research attempts have been made to enhance security by employing trust in network operations.

Modeling trust to enhance security is itself is a separate active area of research. Works like [AH98, GPM04, DVU06, YZV03, OR08, P+11] provide a generic framework to establish and maintain trust relations between nodes in a network. The established trust is later used in better decision making in network activities. The distributed trust model proposed by Rehman et al. [AH98] assumes discrete levels of trust. It employs a decentralized approach to manage trust and a recommendation protocol to exchange trust related information. The model is based on a conditional transitive trust relation that uses trust categories to express trust towards other agents. In order to establish a trust relationship between entities where a direct relation does not exist, the agents can make use of an intermediate agent to establish trust. The various trust models that exist in the literature try to quantify trust relationships according to different applications' security requirements. For example, the PGP style authentication schemes with certification chains [CBH03, ZSF08] use binary trust valuation. Similarly, reputation based schemes such as [OR08, P+11] employ real numbers to measure the trustworthiness of a node.

A dynamic trust updating model in wireless mesh networks [P+13] propose a new dynamic trust updating model (DTUM) in WMNs by taking multiple constraints in to account. This method follows two approaches: 1) The trust increase slowly and drop quickly, similar to the trust relations in human beings. 2) It describes the nature of trust that fades with time.

Trust based security for the OLSR routing protocol [ABS13] propose a trust based solution for securing OLSR protocol in adhoc networks in three steps: Implicit trust relations are analyzed in first step ,then trust based reasoning allow each node to evaluate the behavior of the other nodes as part of second step. Finally, propose mechanism of prevention and countermeasures to resolve inconsistency situations and countering the malicious nodes.

The existing models in the literature can be classified based on how they accomplish three major tasks central to any trust model. The three different tasks are trust establishment, trust maintenance and trust usage. The usage of trust depends on the application and the task it needs to accomplish. For example, trust in PGP style authentication schemes is used to issue and validate certificates whereas trust in networks is mainly used to establish secure paths. In establishing trusted paths, trust is either directly employed to select a path or is integrated with the existing routing metric as in [OR08, P+11]. Trust modeling for ad hoc networks is fairly straight forward as the main focus is on maintaining end-to-end connectivity rather than on enhancing throughput. Hence, trust can be directly employed as a routing metric in ad hoc networks. Works done in this direction include the TAODV protocol proposed in [GPM04] which is a trusted extension to AODV. The path selection process is similar to AODV with trust as the metric rather than hop-count. The trust values of nodes are distributed in prior. To incorporate trust into route selection the route request (RREQ) header is modified to include a trust-level field in the AODV RREQ. When a node receives a RREQ, it rebroadcasts it after modifying the trust level field with the trust value of the node from which it received the RREQ. Every node checks back the re-broadcasted RREQ from its next node to see whether it has provided the proper information. If not, it sends a route warning message questioning the sanctity of the node. The final route selection is based on trust-level metric. The major drawback of this model is the prior distribution of the trust-levels. Moreover, there is no mechanism to modify the established trust-levels depending on the change in nodes' behavior.

But, typical WMN applications like community based mesh networks are supposed to support high throughput internet applications. As the trust value of a node depends only on its past behavior in the network operations and it is accordingly increased or decreased based on the number of successful operations carried out, it is not directly suitable for WMNs. For example, delivering packets successfully is a trust evaluation criterion. In such a case, a packet that is transmitted in a single attempt or after a certain number of retransmissions are considered as a successful event. Therefore, employing trust as the routing metric does not achieve high throughput in WMNs. Initial research attempts in this direction include integrating of trust with the existing routing metric. AODV-REX [OR08] is such an attempt where AODV is extended with a reputation model.

AODV-REX [OR08] is a reputation extension to AODV. In AODV-REX, the reputation of a node is integrated with the hop-count routing metric. Each node maintains two kinds of reputation values for each of its neighbors-local and global. It employs a watchdog to monitor the performance of each of its neighbors. When a node transmits a RREQ, it appends the RREQ with the reputation values of all its neighbors. An intermediate node that receives this broadcasted RREQ, acts on the reputation values of interest and ignores the rest. The RREQ is further appended with the intermediate node's neighbors and retransmitted. The hop-count metric is modified to include the reputation of a node. The basic idea is to create a new virtual distance that takes into account the reputation level of the node connected to the link: the distance of two neighbor nodes increases by decreasing the reputation of one of them. Although, integrating routing metric with trust achieves better performance over trust alone as the routing metric, we will show in the next section that it does not generate optimal routes.

## III. ORTHOGONALITY OF TRUST AND ROUTING METRIC

As discussed in the previous section, employing only trust as the routing metric is not suitable for high performance WMN applications. Integrating trust with the routing metric is an alternative solution, but, in this section, we will show that this option of integrating trust and routing metric does not always deliver optimal performance. As, hybrid wireless mesh protocol (HWMP) is the mandatory routing protocol for IEEE 802.11s Based mesh networks and the air-time link metric (ATLM) is default routing metric, we consider HWMP and ATLM for simplicity. We combine air-time metric of a link with the trust value of a node and show that the attempts to integrate these two variable does not result in optimal performance, and in some cases may form routes through malicious nodes. Our attempts to integrate these two variables are in accordance with the proposed in [OR08]. The trust values of nodes are considered to be real values between the range [0, 1]. A link is preferred over another, if the air-time and trust value of a link $(TV_{La-b})$ are combined in such a way that it offers less effective air-time than the other and a path $\left(\overrightarrow{P_0}\right)$ is said to be free of malicious nodes if it does not include a link (node) with trust values of zero.

**Theorem:** Integrating trust with the routing metric of individual links along a selected path $\left(\overrightarrow{P_0}\right)$ between source **S** and destination **D** does not result into optimal path and may even include nodes that are malicious.

***Proof:*** The proof is based on the argument that integrating two metrics that capture two different aspects of a link cannot be integrated, and if integrated does not always yield optimal results.

Let $P_0$ be the optimal path from the set of paths $\{\overrightarrow{P_l}, \overrightarrow{P_j}, \overrightarrow{P_k}, \overrightarrow{P_0} \ldots \overrightarrow{P_n}\}$ between a source **S** and destination **D** as shown in Fig. 1. The set of links on a path $\overrightarrow{P_0}$ is represented by a set

$$L_{\overrightarrow{P_0}} = \{l_{s-j}, l_{j-k}, l_{k-m} \ldots l_{n-d}\}$$

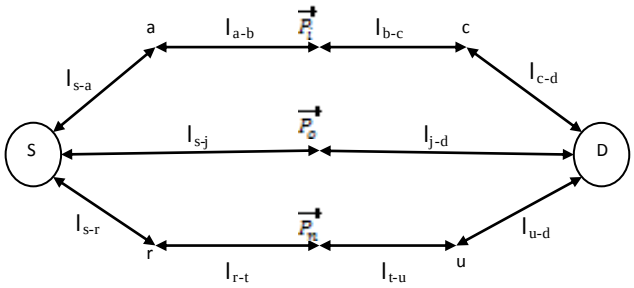


**Fig. 1. Set of paths between source S and destination D**

If $P_0$ is an optimal path, then the cumulative metric offered by individual links in that path are optimal. Therefore, the metric of the path $P_0$, is given by

$$RM\left(\overrightarrow{P_0}\right) = \sum_{Lp_o}\left(l_{s-j(air-time)} \oplus TV_{L_{s-j}}\right) \qquad (1)$$

$$\left(l_{s-j(air-time)} \oplus TV_{L_{s-j}}\right) + \left(l_{j-k(air-time)} \oplus TV_{Lj-k}\right) + \ldots + \left(l_{n-d(air-time)} \oplus TV_{Ln-d}\right)$$

Here, $\oplus$ indicates and operator suitable for integration. As, air-time is the amount of time taken to send a

packet from a node I to J, the trust value of a node can contribute to air-time by reducing the amount of time which is a factor of trust value. That is, if the trust value of a link is high the amount of time is low and vice-versa. For the above metric to be optimal, the RM $(\overrightarrow{P_0})$ does not require all the terms in equation 1 to be optimal, it just requires the RM$(\overrightarrow{P_0})$ to provide best air-time value out of the set of available paths. Without loss of generality, it can be assumed that a link with trust value of zero can be included in the path $\overrightarrow{P_0}$ provided it offers equally better air-time.

Let $\overrightarrow{P_l}$ be an alternate path that exists between the source **S** and destination **D** and has less preferable metric than $\overrightarrow{P_0}$, i.e. $\overrightarrow{P_0}$ offers better air-time than $\overrightarrow{P_l}$, then it can be denoted by,

$$RM\left(\overrightarrow{P_0}\right) < RM\left(\overrightarrow{P_l}\right)$$

$$\sum_{L_{P0}}\left(l_{s-j(air-time)} \oplus TV_{L_{s-j}}\right) < \sum_{L_{P_l}}(l_{s-a(air-time)} \oplus TV_{Ls-a}) \quad (2)$$

$$\sum_{L_{P0}} l_{s-j(air-time)} \oplus \sum TV_{L_{s-j}} < \sum_{L_{P_l}} l_{s-a(air-time)} \oplus \sum TV_{Ls-a} \quad (3)$$

If both the paths $\overrightarrow{P_0}$ *and* $\overrightarrow{P_l}$ have equal air-time then the tie between these paths is decided by the trust metric. That is, the trust metric contributed by $\sum TV_{Ls-j}$ is more than $\sum TV_{Ls-a}$ *therefore,*

$$\sum TV_{L_{s-j}} > \sum TV_{L_{s-a}} \quad (4)$$

For the above equation to be true, the cumulative trust metric offered by $\sum TV_{L_{s-j}}$ should be better than $\sum TV_{L_{s-a}}$.

Preserving the above inequality, the probability of a node/link having a trust value of zero to be included in the selected path $\overrightarrow{P_0}$ without violating the eqn. 4. Therefore, preserving the inequality, a link $l_{k-m}$ in the path $\overrightarrow{P_0}$ is considered to be zero.

$$TV_{l_{s-j}} + TV_{l_{j-k}} + 0 \ldots + TV_{l_{n-d}} > TV_{l_{s-a}} + TV_{l_{a-b}} + TV_{l_{b-c}} + \ldots + TV_{l_{n-d}}$$

This clearly indicates that a node whose trust value of zero is included in the path as the metric considered is cumulative rather than on per-link basis. Hence, a path $\overrightarrow{P_0}$ is selected over a path $\overrightarrow{P_l}$ that is not optimal. This is due to the fact that the two variables that are integrated capture different properties of a wireless link and if integrated does not generate optimal paths.

## IV. THE PROPOSED COMPLEMENTARY TRUST BASED ROUTING

In this section, we present our complementary trust based routing approach to enhance routing security without compromising on throughput. This is achieved with the help of a complementary trust model. The route selection process is driven primarily by the existing routing metric (ATLM). The major advantage of our approach is that it allows the nodes to select a path that offer high-throughput along with the requirement that the nodes that are being chosen satisfy basic trust requirements. This ensures that the nodes in selected path are trustworthy and also offer thigh throughput. The employed trust model contains three different phases of operation that are carried out independently without intervening with the routing process. The trust model provides the nodes with the trust values of its neighbor's that are updated periodically. The three different phases are Initialization, Trust Evaluation and Trust Recommendation.

***Initialization:*** When the network is initialized, each node discovers its neighbors and assigns a trust value of 0.5. A node maintains trust relationships only with its neighbors, i.e. nodes that are in its communication range. The value of 0.5 is justified as node neither trusts nor distrusts a neighbor. The maximum trust value that a node can attain is unity.

***Trust Evaluation****:* Each node periodically evaluates the behavior of each of its neighbors using the trust evaluation procedure. The evaluation procedure is carried out independently by each node and the evaluation timing of nodes need not be synchronized. The evaluation of a neighboring node's behavior is based on the assumption that the all the nodes in the network are fairly loaded. This assumption is justified in a WMN as WMR's are dedicated routers that provide continuous access services to its clients when they are in operational mode. Hence, the contribution of every genuine node in forwarding network traffic is equal. This is not the case in ad hoc networks, where nodes generate data traffic when required. In our trust model, each node monitors the performance of each of its neighbors during an interval of time denoted by $TE_{interval}$. During the time interval $TE_{interval}$, an

evaluator node *I* expects a fixed number of packets ($fp_{ji}$) from each of its neighboring nodes *J* periodically.

An evaluator node *I* also monitors the neighborhood to measure the channel utilization. The main aim of monitoring the utilization of the channel is to keep track of the congestion conditions in the neighborhood. The congestion detection scheme employed is in line with [X+03] that is based on random early detection algorithm (RED) [FJ93]. This allows node *I* to consider losses in the network due to congestion in the neighborhood and avoid penalizing genuine nodes. The number of packets lost due to congestion is estimated and represented by $(\alpha_{ji})$. The trust model also considers the packets that are received in error due to collisions and is represented by $(\beta_{ji})$. At the end of $TE_{interval}$, node *I* calculates the actual number of packets that have been successfully received from a particular neighbor $J$ $(\gamma_{ji})$. The ideal performance by a neighbor is given by eqn. 5

$$fp_{ji} = \alpha_{ji} + \beta_{ji} + \gamma_{ji} \qquad (5)$$

The packets lost due to congestion $(\alpha_{ji})$ are estimated in the following manner. Node *I* continuously monitors its neighborhood to measure the channel utilized. To be more precise, a node *I* will monitor five different radio states 1) Transmitting, 2) Receiving, 3) Carrier sensing busy 4) Virtual carrier sensing busy (e.g. deferral to RTS, CTS etc.) and 5) Idle (i.e., no activity on the channel). These radio states can give an estimate of the node *I*'s contribution and neighborhood contribution to the channel utilization. State 1 & 2 contribute to the node *I*'s channel utilization, states 3 & 4 contribute to the neighborhood contribution, and state 5 is considered as idle time. By monitoring the five radio states, a node can estimate 3 channel utilization ratios, namely total channel utilization ratio (U*busy*), transmitting ratio (U*tx*) and receiving ratio (U*rx*). To determine the channel utilization ratios, a node measures amount of time spent in each channel condition, that are given by T*tx*, T*rx*, T*cs*, T*vcs* and T*idle*. The sum of all the time periods is equal to interval $TE_{interval}$.

The utilization ratios are given by,

$$U_{busy} = \frac{TE_{interval} - T_{idle}}{TE_{interval}} \qquad (6)$$

$$U_{tx} = \frac{T_{tx}}{TE_{interval}} \qquad (7)$$

$$U_{rx} = \frac{T_{rx}}{TE_{interval}} \qquad (8)$$

Using these utilization ratios, one can estimate the size of the neighborhood queue. $U_{tx}$ and $U_{rx}$ give the node *I's* contribution to channel usage. The local drop probability of each node is calculated that is proportional to node's channel bandwidth usage. The dropping probability of the entire neighborhood is determined using eqn. 10 that is derived from the RED congestion algorithm for wired networks that is based on monitoring queue length ($q$) [FJ93]. The terms $max_{th}$ and $min_{th}$ are the maximum and minimum threshold values of the neighborhood queue. The term $max_p$ is the maximum dropping probability achieved when the average queue size reaches the $max_{th}$. The average queue size *avg* is obtained using eqn. 9 where $w_q$ is the queue weight for smoothing the average queue size.

$$avg = (1 - w_q) * avg + w_q * q \qquad (9)$$

$$P_d = \frac{max_p (avg - min_{th})}{(max_{th} - min_{th})} \qquad (10)$$

As node *I* expect equal number of packets from each of its neighbors *J* it determines the dropping probability of a particular neighbor by determining the number of its active neighbors. The values of $\alpha_{ji}$ and $\beta_{ji}$ are estimated and compared with $fp_{ji}$. If the difference in number of packets is not in accordance with $fp_{ji}$ after considering of $\alpha_{ji}$ and $\beta_{ji}$, then the loss in packets is considered to be intentional and the neighboring node is penalized decreasing its trust value by $\delta$ (0.01) for each packet that is lost. If the trust value of a node falls below a threshold value *u* (Upper-Threshold), it requests for a recommendation about that particular neighbor. The evaluation time period can be set accordingly, i.e. it can be longer or shorter depending on the type of application in which the model is employed.

***Trust Recommendation:*** Trust recommendation is an on demand process that is carried out by a node *I* when the trust value of one of its neighbor *J* falls below *u*. All nodes that receive a request for trust recommendation check their respective neighbor list to verify the existence of *J*. If *J* exists in their neighbor list, it replies to the request sent by *I* by sending the current trust value of *J* in its list. Once *I* receive all the recommendations, it re-evaluates the trust value of *J*. If it falls below *l* (Lower Threshold), the neighbor node's status is set to malicious.

## V. ROUTING METHODOLOGY AND SIMULATION ANALYSIS

### *A. Routing Methodology*

The proposed complementary trust mechanism is integrated into HWMP, to enhance its routing security on one-hand and achieving high-throughput on the other. The proposed trust mechanism works at the MAC layer allowing better path discovery process at the network layer. It observes the behavior of each of its neighbors by monitoring the channel utilization conditions. It also does not incur any extra overhead in monitoring the channel as all the channel monitoring states of a node are usually carried out even in the absence of the trust model.

It also allows the routing protocol HWMP to establish secure end-to-end routes by providing it with the observed trust values. The nodes make use of these trust values provided by the trust model to establish secure high throughput routes. In the route discovery process, a source node *O* initiates a route discovery process by broadcasting a RREQ for a destination *D*. An intermediate node *I* that receive a broadcasted RREQ, first verifies the trust value of the transmitter (For example, *O* in the first turn). The RREQ is processed only if the trust value of the transmitter is above a threshold *u* (Upper Threshold), else it is discarded. This process is repeated by each intermediate node until the RREQ reaches the destination or a node that has fairly fresh route to the destination. Finally, when the RREQ reaches the destination *D*, it too verifies the trust value of the transmitter before the uni-casting a RREP through it.The trust model ensures that the nodes that are included in the route pass the basic trust acceptance criteria. Overall the route selection process is mainly driven by the air-time of a link and the trust model complements the route formation by ensuring that the selected nodes satisfy the basic acceptance criteria.

### *B. Simulation Analysis*

This section analyzes the performance of HWMP, when trust is integrated with the air-time routing metric and compare it with the proposed mechanism. We simulated the performance of HWMP built on two different mechanisms. As routing-metric is integrated with trust in the first approach, we have employed the reputation extension model proposed for WMNs [OR08]. In [OR08], the authors have implemented the reputation extension for AODV, but for uniformity we have implemented the same model for HWMP. Moreover as WMNs are high performance access networks, the hop-count metric employed by AODV is not a suitable metric to verify the performance of both the schemes.

The second model is our proposed complementary trust model. Both the trust models are implemented in Omnetpp-4.2.1, a discrete event network simulator. We have considered a mesh backbone network consisting of 48 nodes. The IEEE 802.11s MAC protocol is considered. Malicious nodes are randomly chosen to exhibit malicious behavior by dropping packets. Nodes in the network are allowed to communicate by randomly selecting a source and destination pair. Each node sends a set of packets at any instance of time. The simulation time was set to 2000 seconds. First, we analyze the the packet delivery ratio (PDR) performance of both the protocols along with basic HWMP for both TCP and UDP data traffic as shown in Figure 2 and 3 . The graph Figure 2 and Figure 3 clearly shows that the increase in the total number of packets successfully delivered and increased PDR, when trust is employed independently just to complement the routing metric.

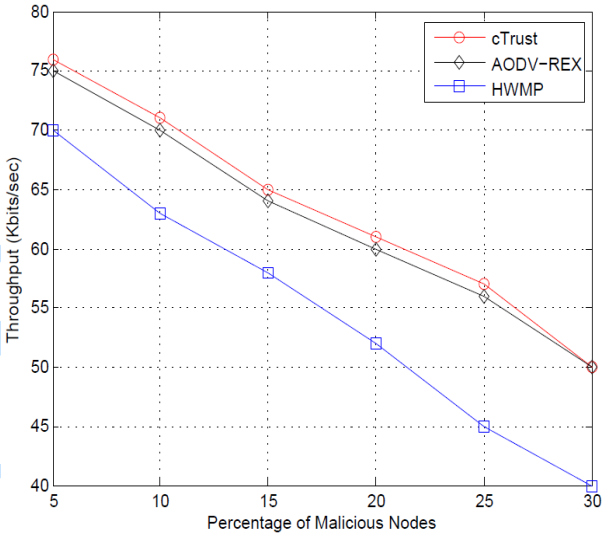


**Fig. 2. TCP Packet Delivery performance of cTrust compared with Aodv-Rex**

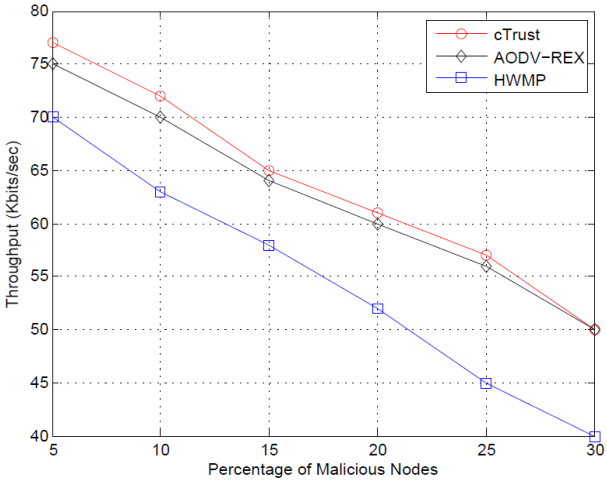


**Fig. 3. UDP Packet Delivery performance of cTrust compared with Aodv-Rex**

Figure 4 shows the overhead analysis of cTrust compared with AODV-REX. cTrust incurs more overhead compared to AODV-REX and HWMP as

it requires additional control packets for sharing trust recommendations with neighboring nodes whereas AODV-REX piggy backs the reputation values in the route request packets. However, AODV-REX incurs high message overhead as each node concatenates the reputation values of all its neighbors while transmitting a route request. Thus, the size of the message grows rapidly as the route request reaches the destination. It also incurs more computation overhead as each node has to process the entire reputation values and their addresses to suitably find the content of interest. Increase in message size also consumes more airtime to transmit a message thus increasing the inter-flow interference.

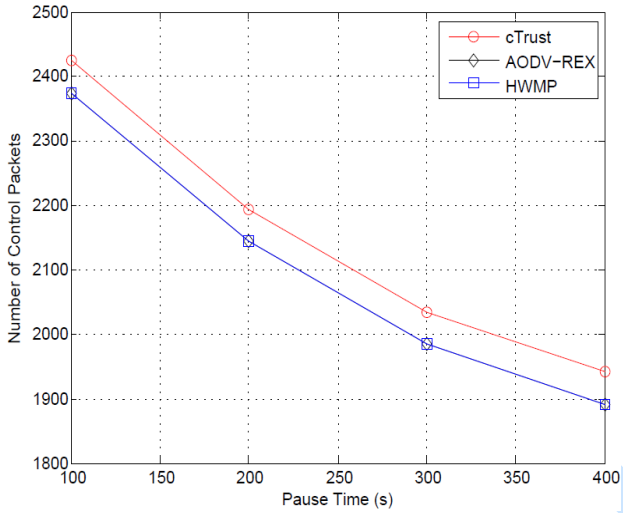


**Fig. 4. Overhead analysis of cTrust compared with Aodv-Rex**

## VI. CONCLUSION

As WMNs are expected to deliver high throughput, either employing only trust for path selection or integration of trust with the underlying routing metric doesn't give optimal performance. The main reason behind this is the independent and the orthogonal nature of the two variables (routing metric and trust). To address this issue, we have developed a complementary trust based routing mechanism that allows nodes to establish paths that are trustworthy and also achieve high throughput (as it is using Airtime metric for path establishment).The proposed trust evaluation mechanism complements the existing routing protocol, HWMP with its trust observations. We have also shown the performance results of both the schemes and verified that the complementary trust based routing approach performs better over integration model.

## REFERENCES

[AH98] **Alfarez Abdul-Rahman, Stephen Halles** - *A Distributed Trust Model*, In Proc. Of New Security Paradigms Workshop, ACM, New York, NY, USA, 1998.

[ABS13] **Asma Adnane,Christophe Bidan, Rafael Timóteo de Sousa Júnior** - *Trust-based security for the OLSR routing protocol*, Computer Communications 36, pp. 1159-117, 2013.

[AWW05] **Ian F. Akyildiz, Xudong Wang, Weilin Wang** - *Wireless mesh networks: A survey*, Computer networks and ISDN systems, 2005.

[Bah07] **Michael Bahr** - *Update on the Hybrid Wireless Mesh Protocol of IEEE 802.11s*, Mobile Adhoc and Sensor Systems, 2007.

[Cou04] **D. S. J. de Couto** - *High-Throughput Routing for Multi-Hop Wireless Networks*, Ph.D. diss., MIT, 2004.

[CBH03] **S. Capkun, L. Buttyan, J. Hubaux** - *Self-organized public-key management for mobile ad hoc networks*, IEEE Transactions on Mobile Computing, vol. 2, no. 1, pp. 52–64, 2003.

[C+03] **D. de Couto, D. Aguayo, J. Bicket, R. Morris** – *A High-throughput path metric for multi-hop wireless routing*. In *MOBICOM*, 2003.

[DPZ04] **R. Draves, J. Padhye, B. Zill** - *Routing in Multi-Radio, Multi-HopWireless Mesh Networks*, ACM MobiCom, pp. 114–28, 2004.

[DVU06] **Kamal Deep Meka, Mohit Virendra, Shambhu Upadhyaya** - *Trust Based Routing Decisions in Mobile Ad-hoc Networks*, In Proc. of the workshop on Secure Knowledge Management (SKM 2006), 2006.

[FJ93] **S. Floyd, V. Jacobson** - *Random early detection gateways for congestion avoidance*, IEEE/ACM Transactions on Networking 1(4):397-413, 1993.

[GPM04] **Tirthankar Ghosh, Niki Pissinou, Kia Makki** - *Collaborative Trust- Based Secure Routing against colluding malicious nodes in Multihop Ad Hoc Networks*, In proc. of 29th Annual IEEE Intl. conference on Local Computer Networks (LCN'04), 2004.

[KB06] **C. E. Koksal, H. Balakrishnan** - *Quality-aware routing metrics for time-varying wireless mesh networks*. Selected Areas in Communications, IEEE Journal on, 24(11), 1984-1994, 2006.

[KHP08] **D. Koutsonikolas, Y. Hu, K. Papagiannaki** - *How to Evaluate Exotic Routing Protocols*, In ACM Hotnets, Calgary, Canada, 2008.

[OR08] **F. Oliviero, S. Romano** – *A reputation-based metric for secure routing in wireless mesh networks*, in Proc. of IEEE GLOBECOM 2008, New Orleans, LA, 2008.

[P+11] **Stefano Paris, Cristina Nita-Rotaru, Fabio Martignon, Antonio Capone** - *EFW: A Cross-Layer Metric for Reliable Routing in Wireless Mesh Networks with Selfish Participants*, in Proc. of IEEE INFOCOMM, Shanghai, China, 2011.

[P+13] **Sancheng Peng, Aimin Yang, Hui Zhong, Ziyuan Feng** - *A dynamic trust updating model based on multiple constraints in wireless mesh networks*, In Information Science and Technology (ICIST), 2013 International Conference on, pp. 815-819. IEEE, 2013.

[SBM06] **P. Subramanian, M. M. Buddhikot, S. C. Miller** - *Interference Aware Routing in Multi-Radio Wireless Mesh Networks, IEEE Wksp. Wireless Mesh Networks*, pp. 55–63, 2006.

[X+03] **K. Xu, M. Gerla, L. Qi, Y. Shu** - *Enhancing TCP fairness in ad hoc wireless networks using neighborhood RED*. In Proceedings of the 9th annual international conference on Mobile computing and networking (pp. 16-28). ACM, 2003.

[YWK05] **Y. Yang, J. Wang, R. Kravets** - *Designing Routing Metrics for Mesh Networks*, IEEE Wksp. Wireless Mesh Networks, 2005.

[YZV03] **Zheng Yan, Peng Zhang, Teemupekka Virtanen** - *Trust Evaluation Based Security Solution in Ad Hoc Networks*, In Proc. of ordic Workshop on SECURE IT, 2003.

[ZSF08] **C. Zhang, Y. Song, Y. Fang** - *Modeling secure connectivity of self organized wireless ad hoc networks*, in Proc. of InfoCom 2008, Phoenix, AZ, April 2008.