# A Node-disjoint Trust-based Multipath Routing Mechanism for Multimedia Sensor Networks

Qian Ye[1], Yufei Wang[2], Yulan Tang[1], Jie Lv[1], Yufang Zhang[1]

[1] Department of Control Technology, Wuxi Institute of Technology, China
[2] Jiangsu Electronic Information Products Quality Supervision Inspection Research Institute, China
qianye11@protonmail.com, yufei.wang27@yahoo.com, yulantang2020@yahoo.com,
jielv29831@outlook.com, yfzhang102192@protonmail.com

## Abstract

Multipath routing is an effective approach to transmit large multimedia data in sensor networks to satisfy the QoS requirements. This paper focuses on QoS-aware trust-based node-disjoint multipath routing mechanism between source node and destination node in two-layer clustered multimedia sensor networks. First, node-disjoint and non-interference logical pipes are created. Then, based on the trust value of single sensor node, single routing path and multiple routing paths, the node-disjoint non-interference routing paths are established. And the update and routing update process is also designed. Finally, the proposed routing method are well simulated. The simulation results show that our QoS-aware trust-based routing mechanism can effectively enhance the packet delivery rate, reduce the packet end-to-end delay, and increase the Peak Signal-to-Noise Ratio.

**Keywords:** Wireless multimedia sensor networks, Trust evaluated, Multipath routing, Logical pipe

## 1 Introduction

Multipath routing is the common mechanism adopted for providing reliability in Wireless Sensor Networks (WSNs) [1], and considered the most effective way to ensure the quality of data service [2]. An Optimized QoS-based clustering with multipath routing protocol for WSNs is proposed to solve energy hole problem [3]. To achieve real-time, reliability requirements of WSNs applications, a routing multipath routing scheme with path bridging to enable cooperation among the paths is proposed in [4]. It is also considered an effective approach to transmit large multimedia data in Wireless Multimedia Sensor Networks (WMSNs) [5]. Multimedia information in WMSNs are usually of rich types and burst. Tight Quality of Service (QoS) requirements in terms of packet losses, delay and jitter is main challenges for WMSNs [5-7]. And multipath routing consisting of different node-disjoint non-correlated paths is a viable solution for the WMSNs [8]. A cross-layer adaptive multipath routing for multimedia wireless sensor networks under duty cycle mode is provided to establish non-correlated and node-disjoint paths form sources to the sink node in [8]. End-to end delay and the energy consumption are the main problems for the WMSNs applications. Multipath routing can satisfy the QoS requirements, but lead to other problems such as multiple paths generation and traffic flow management. The QoS-oriented multipath multimedia transmission planning using multipath routing is designed to solve the problems [9]. There are two reasons for using multipath routing for data transmission in wireless multimedia sensor networks :

(1) the data volume is huge. For example, an I frame can be segmented into several small fragments and transmitted through multiple routing paths;

(2) Reduce the data rate on each path to support applications with high data rate.

Most applications require many WMSNs support quality of service requirements, such as real time limit (must be within a certain period of time to transmit multimedia data to the monitoring centre), and robustness (network can work normally when fault), tamper resistance (network work normally when deliberately attack), prevent hacking (external entities can't hacking into the network multimedia data), the quality of the multimedia information, network transmission quality, energy consumption, quality of network coverage, network service time, as well as the network reliability and fault tolerance, etc. WMSNs are widely used in the field of military and civilian makes it very critical and important security and privacy protection, such as military applications need strong enough security system to cope with all kinds of attacks, and the patient monitoring applications in the field of civil privacy is very important, so to design and build credible WMSNs, research problems and deal with the security and privacy protection, enables the WMSNs to be socially accepted and widely used.

*Corresponding Author: Qian Ye; E-mail: qianye11@protonmail.com
DOI: 10.3966/160792642021012201021

QoS and security is two important factors which influence the application of the WMSNs, and trust management is considered effective to deal with this problem. Trust management has been widely researched in multi-agent systems [10], mobile ad hoc networks [11], ubiquitous networks [12] and sensor networks [13]. Some trust-based multipath routing protocols have been designed for ad hoc networks. A Bayesian statistical model for a multipath trust-based reactive as hoc routing protocol is proposed in [14]. Trust-based on-demand multipath routing framework and protocol are given for mobile ad hoc networks in [15-16]. The trust-enhanced anonymous on-demand routing protocol (TEAP) is proposed to restrain the misuse of anonymity in [17]. Also, lightweight trust management methods or frameworks for medical sensor networks are well studied [18]. Li et al. [19] designs a lightweight and dependable trust system for clustered wireless sensor networks. Feedbacks among cluster members are cancelled, and cluster header with richer resource is responsible for more computing and communication tasks. For fault-tolerant data aggregation in wireless multimedia sensor networks, trust-based framework is designed in [20]. A trust-aware routing framework is designed implemented to secure the WSNs against adversaries misdirecting the multi-hop routing in [21]. A highly scalable cluster-based hierarchical trust management protocol considering multidimensional trust attributes for WSNs is developed in [22] to deal with selfish or malicious sensor nodes. And the protocol is applied for trust-based routing and intrusion detection [22].

However, most researchers in the design or build trust management system based on the trust agreement, tend to focus on the evaluation of a single node or single hop path trust level, and seldom consider trust fusion of multiple routing paths, unable to evaluate by multipath routing protocol to build the routing paths of the overall service quality and level of trust, because of multipath routing is to improve the wireless multimedia sensor network, and multi Agent system, mobile Ad hoc network service quality and reliability of one of the important technical means.

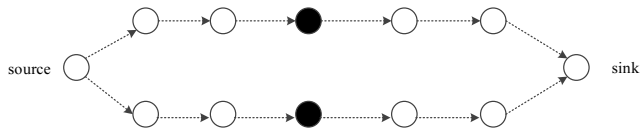
Multipath routes can be used in wireless multimedia sensor networks to transmit video, image, and other multimedia information. The benefits include balancing network load, improving the average network capacity to ensure the quality of multimedia transmission service and balancing energy consumption to avoid single point failure. On the other hand, as an important supplement of cryptography, trust management can be used to resist internal attacks, identify malicious and selfish nodes, and improve the security, reliability, and fairness of wireless sensor networks. Furthermore, the QoS guarantee trust management can be used to comprehensively evaluate the trusted QoS guarantee level of multi-path routing, and can provide the basis and reference for multi-path routing update and load balancing. The main factors to measure QoS demand of multimedia sensor network include link bandwidth, delay, packet loss rate, energy consumption, delay jitter and so on. And these factors should be satisfied in multipath routing.

Considering that the data transmission efficiency and reliability of multipath routing are higher without shared nodes and communication links, most multipath routing protocols are designed to be disjoint and interference free. On the other hand, most of the researchers focus on evaluating the trust level of single node or single routing path; few consider the trust computing of multipath routing which is effective approach to guarantee the QoS in WMSNs. Consequently, based on the QoS-aware trust management, a node-disjoint and interference-free multipath routing mechanism for multimedia sensor networks is designed in this paper.

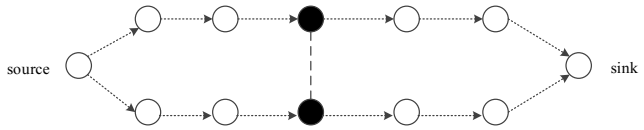
## 2 Node-disjoint Trust-based Multipath Routing

### 2.1 Multipath Routes

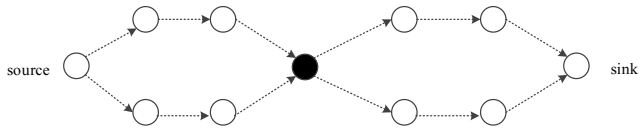
The multi-path routing mechanisms from the source node to the destination node can be divided into two types: node disjoint and node joint. Node-disjoint routing refers to the multi-hop routing paths that does not share the routing node. And node-disjoint multipath routing can be link disjoint or node disjoint [23], where node disjoint is further divided into edge-connected and 0-edge-connected. Figure 1 shows an example of three types of multipath routes.




(a) node-disjoint、0-edge-connected




(b) node-disjoint、edge-connected




(c) with common modes

**Figure 1.** Examples of Multipath Routing

In this section, routing mechanism is proposed to establish the disjoint and non-interfering trusted

multiple routing paths between source node and sink node. It is assumed that the deployed wireless multimedia sensor network is a two-layer clustering topology. All cluster-head nodes and sink nodes constitute the backbone network. The nodes within the backbone network and those in the common cluster have different communication frequency bands, so there is no interference between them.

In the network topology of two-layer clustering multimedia sensor network, multimedia sensor nodes are grouped into clusters. Nodes with more abundant resources in each cluster are called cluster heads. All ordinary multimedia sensor nodes belonging to different clusters form the bottom layer. The cluster-head node forms the second layer network and is responsible for transmitting the data of each cluster to the destination node. A multi-hop routing path is established between each cluster and sink node through disjoint multi-path routing. Multimedia data generated by ordinary multimedia sensor nodes are first transmitted to the cluster head, and then transmitted to the sink node through multiple non-intersecting routing paths (backbone network formed by cluster heads) without interference.

According to the network topology of two-layer clustering multimedia sensor network, the multipath routing is formed through two stages. First, the multimedia data generated by the common nodes within the cluster are transmitted to the cluster-head node through multiple routing paths. Then, the cluster-head transmits the received multimedia data to the sink node through the multiple routing paths of backbone network. Considering the above two routing processes are similar, we abstract the problem as the multipath routing between the source node and the destination node. Obviously, it is also applicable to both intra-cluster multi-path routing and backbone multi-path routing.

## 2.2 Example of the Node-disjoint and Non-interference Multipath Routing Topology

Suppose each node in a densely deployed multimedia sensor network can perceive its own position and other neighbour nodes within its communication range. Figure 2 shows an example of node-disjoint and non-interfering multipath routing topology. The parameter "R" in Figure 2 is the communication diameter of the nodes. And The physical distance between logical pipes are equal to the communication radius of the nodes, which ensures that the three routing paths will not interfere with each other on the communication channel.

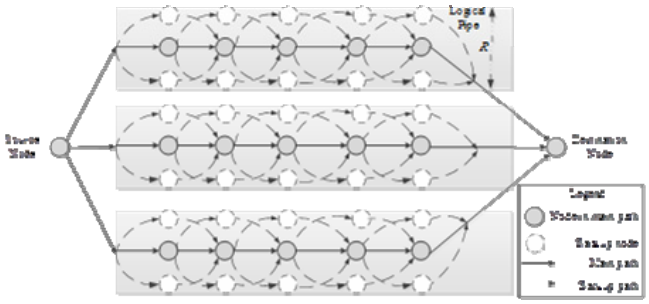


**Figure 2.** Node-disjoint and Non-interference Multipath Routing Topology between Source node and Destination Node

As shown in Figure 2, three node-disjoint routing paths is established between the source node and the destination node. And the three route paths are in three logical pipelines respectively. And the physical distance between neighbour logical pipes is set equal to the communication radius of nodes to ensure the three route paths cannot interfere each other.

For multipath routing, if any path fails, it needs to restart path updating and recovery process, which results in a large consumption of network resources. In view of this, we set up backup for each node of the main routing path within each logical pipeline, so that it can be restored quickly when a node on the path fails or is damaged. Backup nodes can also be used to switch between the main path and the backup path, to maintain the service quality of the routing path and improve the life cycle of multi-path routing.

## 2.3 Node-disjoint and Non-interference Logical Pipes

The main parameters used in the formulas in this section are listed in Table 1.

Before the logic pipeline is established, the number of routing paths need to be determined according to the QoS requirements and network status of multimedia sensor network. Let the expected quality of service of the application is $qos$, the reliability requirement is $rq$, the real-time requirement is $hq$, and the channel error rate is $ber$. Then, we can get the probability that the packet reaches the destination node after $hq$ hop:

$$p_{hq} = (1 - ber)^{hq} \quad \textbf{(1)}$$

In order to forward $m$ packets successfully, $nm$ paths are needed to guarantee the reliability $rq$, and at least $m$ paths within the $nm$ paths to be able to be used for data transmission. If each path has the same hops, the probability of successful transmission is $p_{hq}$, and the probability of unsuccessful transmission is $1 - p_{hq}$, which follows the Bernoulli distribution:

**Table 1.** Main Parameters used in the Formulas

| Sr. No | Parameter | Description |
|---|---|---|
| 1 | $rq$ | the probability that a packet is successfully delivered to the destination node |
| 2 | $qos$ | the expected quality of service of the application |
| 3 | $hq$ | the hops of the routing path |
| 4 | $ber$ | the channel error rate |
| 5 | $m$ | number of packets needed to successfully forward<br>number of paths able to be used for data transmission |
| 6 | $nm$ | Number of paths |
| 7 | $p_{hq}$ | the probability of successful transmission |
| 8 | $1-p_{hq}$ | the probability of unsuccessful transmission |

$$\begin{aligned} rq &= \sum_{i=0}^{m} C_{nm}^{i}(1-p_{hq})^{nm-i}\, p_{hq}{}^{i} \\ &= \sum_{i=0}^{m} C_{nm}^{i}(1-(1-ber)^{hq})^{nm-i}(1-ber)^{hq*i} \end{aligned} \tag{2}$$

The normal distribution method can be used to approximate the number of multipath routes, that is, the value of $m$.

Mean value $\mu = nm(1-\mathrm{ber})^{hq}$

Variance $\sigma^2 = nm(1-ber)^{hq}(1-(1-\mathrm{ber})^{hq})$

For the standard normal distribution, $P(\mathrm{n} \geq \mathrm{nr}) \geq \mathrm{rq}$, where $m \leq n \leq nm$ and $nr$ represents the minimum path quantity satisfying rq . According to the properties of normal distribution, we use the following formula to get the value of $m$:

$$\begin{aligned} m = nr*\sigma+\mu = nr*\sqrt{nm(1-ber)^{hq}(1-(1-\mathrm{ber})^{hq})} \\ + nm(1-ber)^{hq} \end{aligned} \tag{3}$$

In which, $nr*\sigma+\mu$ represents the expectation of the normal distribution.

We assume that nodes can identify the locations of neighbor nodes and themselves using location algorithm or GPS information. And the location of sink node is known for entire network. The location of the cluster head nodes is shared within the cluster. Then, we take the source node and destination node as central axis and divide the logical pipeline according to the required number of disjoint routing paths. Then, we set the distance between the boundaries of adjacent logical pipelines as the communication radius of nodes (if more logical pipelines are needed, the communication radius can be reduced by reducing the transmitted power), to ensure no interference between nodes in different logical pipelines. The method in reference [24] can be applied to establish the logical pipeline.

## 2.4 Trust Management and Fusions

For sensor nodes in routing path, the trust value is calculated based on packet-drop-rate, residual-energy, and the queue length of the sensor node. Monitoring packet dropping can help identify malicious and selfish nodes, so we use packet drop rate to evaluate the node's trust value. In order to simplify and reduce the load on resource-constrained wireless multimedia sensor networks, we only passively monitor the delivered packets to evaluate trust values. The Beta distribution has been shown to be effective in describing the binomial distribution at each time unit by calculating the trust value based on the packet delivery rate by the number of packets successfully delivered. Resource constraint is a major challenge faced by wireless sensor networks, and residual energy is one of the key factors to measure the node trust level, which determines whether the node can provide continuous service capability in the future. Delay is an important QoS guarantee requirement for wireless multimedia sensor network application. The queuing time of data packets at the relay node is a key factor affecting the end-to-end delay of data packets, and the forwarding waiting time of data packets at the relay sensor node can be measured by the occupancy of queue buffer. Specific calculation methods for single sensor trust value is described in [25].

From Table 2 the mapping relationship between MOS, PSNR and trust values based on packet loss rate can be approximated. Especially for video streaming transmission, routing path of packet loss rate directly affect the final quality of video transmission, to assess the video quality of two important parameters for the Peak signal-to-noise Ratio PSNR and average Opinion value MOS, usually, the smaller the packet loss rate, the greater the PSNR and MOS value, as a result, for the user, based on the trust of the packet loss rate value reflects the user right by the path's expectations of the transmission of video quality, Objective mapping relationship between the trust value based on packet loss rate and PSNR and MOS.

The main parameters used in the formulas in section 2.4 are listed in Table 3.

The state of the routing path includes the interference of the relay node, the residual energy of the node, the backlog of traffic on the path and so on. Therefore, in our proposed trust fusion mechanism, the trust level of routing path state is calculated through data delivery rate, node residual energy and packet transmission delay. Methods of QoS-aware trust

**Table 2.** The mapping relationship between MOS, PSNR and trust values based on packet loss rate

| Sr. No | MoS | PSNR | Trust Values based on packet loss rate |
|---|---|---|---|
| 1 | 5 (Perfect) | greater than or equal to 30dB | greater than or equal to 0.95 |
| 2 | 4 (good) | greater than or equal to 29dB, less than 30dB | greater than or equal to 0.9, less than 0.95 |
| 3 | 3 (Fair) | greater than or equal to 27dB, less than 29dB | greater than or equal to 0.85, less than 0.9 |
| 4 | 2 (Poor) | greater than or equal to 25dB, less than 27dB | greater than or equal to 0.75, less than 0.85 |
| 5 | 1 (Bad) | less than 25dB | less than 0.75 |

**Table 3.** Main Parameters used in Section 2.4

| Sr. No | Parameter | Description |
|---|---|---|
| 1 | $Q_1$ | $packet\text{-}drop-rate$ |
| 2 | $Q_2$ | $residual-energy$ |
| 3 | $Q_3$ | $time-delay$ |
| 4 | $Q=\{Q_1,Q_2,Q_3\}$ | QoS requirements |
| 5 | $V$ | set of nodes in deployed WMSNs |
| 6 | $MR$ | multipath routing consists of $n\geq 1$ node-disjoint routing paths |
| 7 | $MP^n=\{P_1,P_2,\cdots,P_n\}$ | a collection of disjoint paths from a source node to a destination node |
| 8 | $v_i^m(1\leq m\leq k)\in V$ | relay nodes |
| 9 | $v_s$ | source node |
| 10 | $v_d$ | destination node |
| 11 | $P_i^{(k)}=(v_s,v_i^1,\cdots,v_i^k,v_d)$ | the $i^{th}$ route path |
| 12 | $T$ | the lifetime of the established routing path |
| 13 | $\Delta t_r$ | equal time window |
| 14 | $0<trust_{i,j}(\Delta t_r)<1$ | the trust value of the QoS requirement $Q_j$ based on $i^{th}$ single routing path $P_i^{(k)}$ at the end of $i^{th}$ time window $\Delta t_r$ |
| 15 | $Trust_{\Gamma,j}(\Delta t_r)$ | the "fused trust" of the QoS Requirement $Q_j$ at the end of $r^{th}$ the time window based on a subset $\Gamma\in(Power$ set of $MP^n)$ of routing paths |
| 16 | $RESIDUAL\_Er(v_i^m)$ | the residual energy of sensor node $v_i^m$ |
| 17 | $FULL\_Er(v_i^m)$ | the initial full energy of sensor node |
| 18 | $OCCUPY\_Len(v_i^m)$ | the length of the occupied receiving and sending buffer queues on relay node $v_i^m$ |
| 19 | $BUFFER\_Len(v_i^m)$ | the full length of receiving and sending buffer queues on $v_i^m$ |

evaluation for multipath routing is detailed in reference [25].

For a single routing path $P_i^{(k)}=(v_s,v_i^1,\cdots,v_i^k,v_d)$, data are delivered from source node $v_s$ to the destination sink node $v_d$ through $k$ relay sensor nodes. The number of relay nodes and the trust value of the relay nodes are evaluation parameters of the trust level of the routing path. According to "trust propagation does not increase trust" and "Information does not increase by propagation", the trust value of the routing path should not be higher than the trust value of the relay node.

For specific multimedia sensor network applications, the routing path might satisfy one or multiple QoS requirements. In order to evaluating the comprehensive trust level of single routing path considering multiple QoS requirements, we fuse the trust value through the follow equations:

$$trust_i(\Delta t_r)=\eta_1\times trust_{i,1}(\Delta t_r)+\eta_2\times trust_{i,2}(\Delta t_r)+\eta_3\times trust_{i,3}(\Delta t_r) \quad \textbf{(4)}$$

Where,

$$trust_{i,1}(\Delta t_r)=\prod_{m=1}^{k}\left(trust_{(v_i^m,1)}(\Delta t_r)\right)$$

is the trust value of the packet-drop-rate based on routing path $P_i^{(k)}$ at time period $\Delta t$;

$$trust_{i,2}(\Delta t_r)=MIN[trust_{(v_i^1,2)}(\Delta t_r),\cdots,trust_{(v_i^k,2)}(\Delta t_r)]$$

is the trust level of single routing path based on residual-energy;

$$trust_{i,3}(\Delta t_r)=1-\frac{\sum_{m=1}^{k}OCCUPY\_Len(v_i^m)}{\sum_{m=1}^{k}BUFFER\_Len(v_i^m)}$$

is the trust level of the single routing path based on packet delivery queue length.

$0 \le \eta_1 \le 1$, $0 \le \eta_2 \le 1$ and $0 \le \eta_3 \le 1$. The value of $\eta_1$, $\eta_2$ and $\eta_3$ can be adjusted considering different QoS requirements of applications. In particular, if $trust_{i,2}(\Delta t_r) = 0$, then $trust_i(\Delta t_r) = 0$. This means that if a path has an energy trust value of 0, the routing path will be invalidated.

Before fusing the trust values of multiple disjoint routing paths, we give the following two assumptions:

Hypothesis 1: Assume that the overall trust value of a single routing path is greater than 0.5;

Hypothesis 2: The trust values of multiple routing paths are independent of each other because multiple routing paths are non-intersecting and non-interfering.

Based on the above two assumptions, we can conclude that when more trusted paths are added, the overall trust value of a set of routing paths increases monotonically.

Trust fusion is the process of calculating the overall trust value of a group of routing paths, and each routing path in the group is node disjoint, has no interference with each other, and has its own trust value.

First, we compute the overall trust value of two node-disjoint routing paths. Given two routing path $P_i \in MP^n$ and $P_l \in MP^n$ have their own trust value $trust_{i,j}(\Delta t_r)$ and $trust_{l,j}(\Delta t_r)$ for the QoS requirement $Q_j$ at the end of time period $\Delta t_r$ respectively. We use a Bayesian method to fuse the trust values of the two routing paths. The overall trust value $Trust_{\Phi,j}(\Delta t_r)$ for the QoS requirement $Q_j$ at the end of time period $\Delta t_r$, in which $\Phi = \{P_i, P_l\}$, is computed as follows:

$$Trust_{\Phi,j}(\Delta t_r) = \frac{trust_{i,j}(\Delta t_r) \times trust_{l,j}(\Delta t_r)}{trust_{i,j}(\Delta t_r) \times trust_{l,j}(\Delta t_r) + \left(1 - trust_{i,j}(\Delta t_r)\right) \times \left(1 - trust_{l,j}(\Delta t_r)\right)} \quad (5)$$

Then, the overall trust value is iteratively computed for the $n$ node-disjoint paths $MP^n = \{P_1, P_2, \cdots, P_n\}$. Let $Trust_{MP^{i-1},j}(\Delta t_r)$ be the overall trust of a group of $i-1$ routing paths $MP^{i-1} = \{P_1, P_2, \cdots, P_{i-1}\}$ for the QoS requirement $Q_j$ at the end of time period $\Delta t_r$. By fusing the trust value $trust_{i,j}(\Delta t_r)$ of routing path $P_i \in MP^n$ with $Trust_{MP^{i-1},j}(\Delta t_r)$, the overall trust value $Trust_{MP^i,j}(\Delta t_r)$ of a group of $i$ paths $MP^i = \{P_1, P_2, \cdots, P_{i-1}, P_i\}$ for the QoS requirement $Q_j$ at the end of time period $\Delta t$ is computed as:

$$Trust_{MP^i,j}(\Delta t_r) = \frac{Trust_{MP^{i-1},j}(\Delta t_r) \times trust_{i,j}(\Delta t_r)}{Trust_{MP^{i-1},j}(\Delta t_r) \times trust_{i,j}(\Delta t_r) + \left(1 - Trust_{MP^{i-1},j}(\Delta t_r)\right) \times \left(1 - trust_{i,j}(\Delta t_r)\right)} \quad (6)$$

## 2.5 Establish Process of Node-disjoint and Trust-based Routing

The multipath logic pipeline can ensure that there is no interference among multipath routes and nodes. In each logical pipeline, only nodes located in the logical pipeline are selected as the next hop for data transmission. The next hop node is selected according to the trust value of the node. And the backup routing path is established considering the trust value of other nodes in the pipeline. The destination node evaluates the fusion trust values of the nodes in each logical channel and feed back to the logical channel. The destination node also performs a comprehensive trust evaluation on all routing paths to determine whether the required QoS is met or not.

The establishment process of node-disjoint and trust-based multipath routing is as follows:

(1) According to the requirements of application service quality, the number of logical channels from the source node to the cluster-head node within the cluster and the number of logical channels from the cluster-head node to the sink node all need be determined first using the method described in section 2.2, and then the logical channels are established respectively.

(2) Initializes and computes the trust value for each node in the network using the methods introduced in [25]. Specifically, the nodes store the trust values of themselves and their neighbors; the cluster-head node is responsible for managing and maintaining the trust values of all nodes in the cluster; and the sink node is responsible for managing and maintaining the trust values of all cluster-head nodes.

(3) Along the direction from the entrance node of the logical pipeline to the destination node, the current node selects the node with the largest trust value as the next hop, and establishes the next hop backup node in the current node routing table (the trust value can be sorted according to the specific situation of the neighbor node as the priority of the backup node).

(4) Step (3) is performed on all logical channels between the source and destination nodes.

(5) According the methods described in section 2.4, The destination node calculates the trust value of the backbone routing path in each logical pipe using the Algorithm 1 in [25].

(6) After routing paths within all logic pipelines are established, the trust value of the established multiple paths can be computed according the methods described in section 2.4.

And the destination node makes a comprehensive judgment on the trust value of disjoint multiple routing

paths formed, to determine whether the established multipath route meets the quality of service requirements. And then, we establish a set of routings that satisfy the quality of service and discard the logical pipeline that has a negative contribution to the overall trust value. The specific steps are shown below:

It is assumed that the application requirement for the trust value in the multimedia sensor network is $Trust\_qos$, and the comprehensive trust value of the backbone routing path in the logical pipeline is $PathTrust$.

If $PathTrust < Trust\_qos$, it means that this path has a negative contribution to the comprehensive trust value of the entire disjoint multipath route. In this case, the logical pipeline where the path is located is directly abandoned.

For the routing paths $PathTrust \geq Trust\_qos$, we calculate its comprehensive trust value according to the multiple routing paths trust fusion method.

The destination node feeds back to the source node the set of trusted logical channels with values greater than $Trust\_qos$.

(7) The source node selects the trusted logical channel for packet delivery according to the set of trusted logical channels feedback from the destination node and the priority of multimedia traffic packets.

### 2.6 Update Process of Node-disjoint and Trust-based Routing

Routing update is divided into two steps: backbone path of logical pipeline update and multipath update.

The update process of the backbone path route within the logical pipe follows the steps below:

(1) The nodes located on the backbone path periodically assess the trust value of its neighbor node. If the trust value of the next-hop node on the current path is less than the value of the backup node on the same path, the backup node with the maximum trust value is set as the next hop, and the latest trust value of the next-hop node is feedback to the destination node. The destination node then reevaluates the trust value for the whole path.

(2) If the updated trust value of backbone path in the logical pipe is less than, the logical pipe will be discarded directly.

The update process of the multi-path route follows the steps below:

(1) If the backbone path route in the logical pipe is updated, the destination node calculates its updated trust value.

(2) If the updated trust value of the backbone path route is less than $Trust\_qos$, first update the trusted logical pipeline set, then delete the previous logical pipeline from the set, and feedback the latest trusted logical pipeline set to the source node.

(3) If the multimedia sensor network application needs to improve the value of $Trust\_qos$, we only need to re-adjust the set of trusted logic pipelines, then delete those logical pipelines that do not meet the application requirements, and feed the latest set of trusted logic pipelines back to the source node.

(4) If the multimedia sensor network application needs to reduce the value of $Trust\_qos$, we can also simply add those that satisfy the current $Trust\_qos$ to the set of trusted logic pipelines.

## 3 Simulation

We simulate and evaluate the performance of the proposed trust-based node-disjoint routing algorithm in NS2, and the network topology was created as Figure 2. We compared and analyzed the model proposed in this paper with existing disjoint multipath routes, such as EDM [26], RDGM [24], LDMR [27], and used video transmission test sequence foreman (select different routing paths for different frames) in the following data analysis and comparison. The main network simulation parameters are listed in Table 4.

**Table 4.** Main Simulation Parameters

| Sr. No | Parameter | Value |
|---|---|---|
| 1 | Number of node-disjoint multipath routes | 2, 3, 4, 5, 6, 7, 8 |
| 2 | Number of nodes | 300 |
| 3 | Node deployment | Random uniform distribution |
| 4 | Number of backup relay nodes | 2 |
| 5 | MAC | 802.11 DCF |
| 6 | Simulation time | 600sec |
| 7 | Source traffic type | CBR and foreman video sequence |
| 8 | Packet size | 512 |
| 9 | Transmit power | 0.7w |
| 10 | Received power | 0.4w |
| 11 | Idle power | 0.3w |
| 12 | Node initial energy | 10J |
| 13 | Node queuing model | FIFO |
| 14 | Node initial trust value | 1 |
| 15 | Size of scene | 600m*600m |
| 16 | Node communication range | 50m |

Figure 3 and Figure 4 shows the performance of different routing mechanisms.

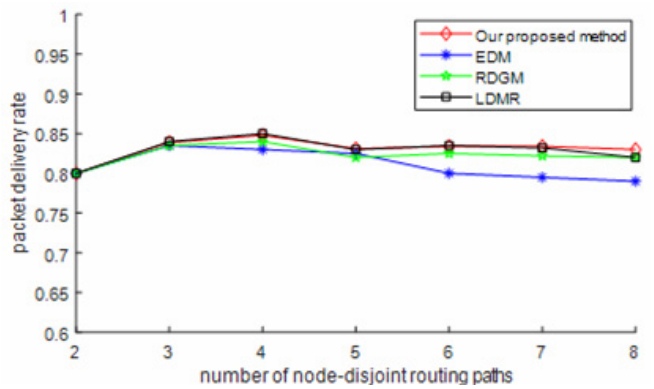



**Figure 3.** Packet Delivery Rate

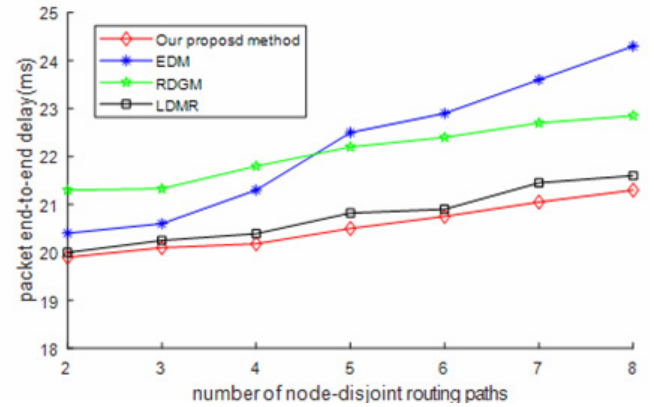



**Figure 4.** Packet End-to-end Delay

As shown in Figure 3, with the increasing of the node-disjoint routing path number, the proposed routing mechanism and LDMR [27] have the higher packet delivery rate. However, when the number of disjoint routing paths is greater than 4, the packet delivery rate will not increase with the increasing of routing paths, which reflects that in the case of a certain network size, excessive routing paths will reduce data transmission performance. In this paper, the number of disjoint logic channels required can be calculated according to the QoS requirements of multimedia sensor network applications.

As shown in Figure 4, the proposed routing mechanism has the minimum packet end-to-end delay. This is because the most QoS-trusted routing paths will be selected to deliver the packets in our routing mechanism, and the queue in buffer of the relay nodes is an important metric parameter.

Then, we set the number of multipath routes as 3, and observe the mean PSNR (Peak Signal-to-Noise Ratio) of different disjoint multipath routes under different number of video sources. All video packets have the same priority.

As shown in Figure 5, we get the average PSNR value of video frames obtained by sink nodes. And the PSNR value using our approach is the best, because each relay node has two backup nodes during the establishment of multipath routing. When the traffic load increases continuously, the relay node and backup node can switch with each other according to the change of node trust value, which ensures the credibility and reliability of the routing path.

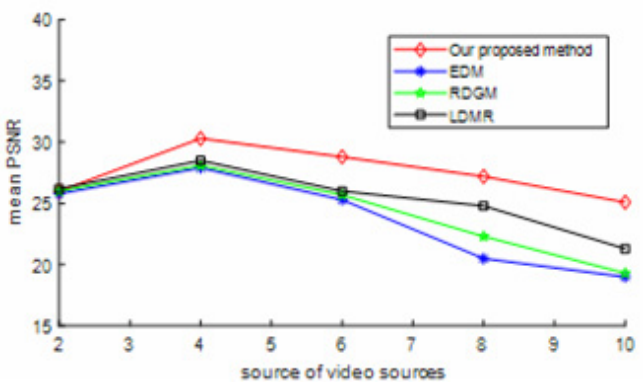



**Figure 5.** PSNR (Peak Signal-to-Noise Ratio)

## 4 Conclusions

In this paper, we propose a node-disjoint multipath routing mechanism for multimedia sensor networks, and the trust value is evaluated considering QoS factors, such as packet-delivery-rate, residual energy of nodes and time delay of packet delivery. Based on the QoS-aware trust computation, we developed mechanisms for trust-based routing in two-layer clustered multimedia sensor networks. The designed node disjoint security trusted multipath routing method is based on node-disjoint non-interference logic pipeline and multi-path routing QoS-aware trust fusion. According to simulating the algorithms, we concluded that our methods can afford an effective and secure QoS-aware reference for designing multipath routing.

Multi-path routing trust fusion can effectively evaluate the performance of multi-path routing trusted QoS guarantee and provide reference for multi-path routing traffic scheduling and load balancing. Energy consumption may be the main shortages in the process of non-interference logic pipeline establishment and trust value calculation. In the future, the trusted node disjoint routing protocol suitable for multimedia sensor networks will be further developed considering the energy consumption problem.

## Acknowledgements

In this paper, the research was sponsored by the 333 Project in Jiangsu Province of China under Grant No. BRA2018317.

## References

[1] S. Misra, M. Reisslein, G. Xue, A survey of multimedia

streaming in wireless sensor networks, *IEEE Communications Surveys & Tutorials*, Vol. 10, No. 4, pp. 18-39, Fourth Quarter, 2008.

[2] X. Fu, Y. Yang, O. Postolache, Sustainable Multipath Routing Protocol for Multi-Sink Wireless Sensor Networks in Harsh Environments, *IEEE Transactions on Sustainable Computing*, doi: 10.1109/TSUSC.2020.2976096, February, 2020.

[3] O. Deepa, J. Suguna, An optimized QoS-based clustering with multipath routing protocol for Wireless Sensor Networks, *Journal of King Saud University - Computer and Information Sciences*, Vol. 32, No. 7, pp. 763-774, September, 2020.

[4] S. Kim, C. Kim, K. Jung, Cooperative multipath routing with path bridging in wireless sensor network toward IoTs service, *Ad Hoc Networks*, Vol. 106, 102252, September, 2020.

[5] I. F. Akyildiz, T. Melodia, K. R. Chowdhury, A survey on wireless multimedia sensor networks, *Computer Networks*, Vol. 51, No. 4, pp. 921-960, March, 2007.

[6] O. B. Akan, P. Frossard, Q. Zhang, N. Jayant, Guest Editorial: Special issue on wireless multimedia sensor networks, *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Vol. 52, No. 13, pp. 2529-2531, September, 2008.

[7] L. Atzori, T. Dagiuklas, C. Politis, Special issue on multimedia over ad-hoc and sensor networks, *Mobile Networks and Applications*, Vol. 13, No. 3-4, pp. 243-245, August, 2008.

[8] I. Jemili, D. Ghrab, A. Belghith, M. Mosbah, Cross-layer adaptive multipath routing for multimedia Wireless Sensor Networks under duty cycle mode, *Ad Hoc Networks*, Vol. 109, 102292, December, 2020.

[9] M. S. Hossain, X. You, W. Xiao, J. Lu, E. Song, QoS-oriented multimedia transmission using multipath routing, *Future Generation Computer Systems*, Vol. 99, pp. 226-234, October, 2019.

[10] H. Yu, Z. Shen, C. Leung, C. Miao, V. R. Lesser, A Survey of Multi-Agent Trust Management Systems, *IEEE Access*, Vol. 1, pp. 35-50, May, 2013.

[11] K. Govindan, P. Mohapatra, Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey, *IEEE Communications Surveys & Tutorials*, Vol. 14, No. 2, pp. 279-298, Second Quarter, 2011.

[12] A. Ladas, D. G. C., N. Pavlatos, C. Politis, A Selective Multipath Routing Protocol for Ubiquitous Networks, *Ad Hoc Networks*, Vol. 77, pp. 95-107, August, 2018.

[13] S. M. Zin, N. B. Anuar, L. M. Kiah, I. Ahmedy, Survey of secure multipath routing protocols for WSNs, *Journal of Network & Computer Applications*, Vol. 55, pp. 123-153, September, 2015.

[14] Y. Begriche, H. Labiod, a bayesian statistical model for a multipath trust-based reactive ad hoc routing protocol, *2009 7th International Conference on Information, Communications and Signal Processing (ICICS)*, Macau, China, 2009, pp. 1-8.

[15] C. Qu, L. Ju, Z. Jia, H. Xu, L. Zheng, Light-Weight Trust-Based On-Demand Multipath Routing Protocol for Mobile Ad Hoc Networks, *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Melbourne, VIC, Australia, 2013, pp. 42-49.

[16] H. Xia, Z. Jia, L. Ju, X. Li, E. H.-M. Sha, Impact of trust model on on-demand multi-path routing in mobile ad hoc networks, *Computer Communications*, Vol. 36, No. 9, pp. 1078-1093, May, 2013.

[17] M. Gunasekaran, K. Premalatha, TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks, *IET Information Security*, Vol. 7, No. 3, pp. 203-211, September, 2013.

[18] D. He, C. Chen, S. Chan, J. Bu, A. V. Vasilakos, ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks, *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 4, pp. 623-632, July, 2012.

[19] X. Li, F. Zhou, J. Du, LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 6, pp. 924-935, June, 2013.

[20] Y. Sun, H. Luo, S. K. Das, A Trust-Based Framework for Fault-Tolerant Data Aggregation in Wireless Multimedia Sensor Networks, *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 6, pp. 785-797, November-December, 2012.

[21] G. Zhan, W. Shi, J. Deng, Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs, *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 2, pp. 184-197, March-April, 2012.

[22] F. Bao, I.-R. Chen, M. Chang, J.-H. Cho, Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, *IEEE Transactions on Network and Service Management*, Vol. 9, No. 2, pp. 169-183, June, 2012.

[23] S. Waharte, R. Boutaba, Totally Disjoint Multipath Routing in Multihop Wireless Networks, *2006 IEEE International Conference on Communications (ICC '06)*, Istanbul, Turkey, 2006, pp. 5576-5581.

[24] J. Lee, H. Park, S. Oh, Y. Yim, S.-H. Kim, A Radio-disjoint Geographic Multipath Routing in Wireless Sensor Networks, *2012 26th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, Fukuoka, Japan, 2012, pp. 803-809.

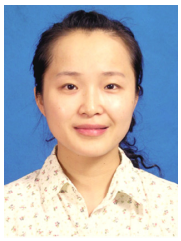
[25] Q. Ye, M. Wu, Y. Wang, A QoS-aware Trust Model for Multipath Load Balancing in Multimedia Sensor Networks, *Journal of Software Engineering*, Vol. 9, No. 1, pp. 50-65, January, 2015.

[26] H. W. Oh, J. H. Jang, K. D. Moon, S. Park, E. Lee, S.-H. Kim, An explicit disjoint multipath algorithm for Cost efficiency in wireless sensor networks, *2010 21st IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Istanbul, Turkey, 2010, pp. 1899-1904.

[27] K. Jung, E. Lee, S. Oh, Y. Yim, S.-H. Kim, Localized disjoint multipath routing protocol in irregular wireless sensor networks, *2013 24th IEEE International Symposium on*

*Personal, Indoor, and Mobile Radio Communications (PIMRC)*, London, UK, 2013, pp. 2454-2458.

## Biographies



**Qian Ye** received the Ph.D. degree at Nanjing University of Posts and Telecommunications, China. She is currently with Department of Control Technology, Wuxi Institute of Technology, China. Her current research interests include Sensor Network and Information Security.

**Yufei Wang** received the Ph.D. degree from Nanjing University of Posts and Telecommunications, China. He is currently working in Jiangsu Electronic Information Products Quality Supervision Inspection Research Institute, China. His current research intersets inlucde industril control system and security.

**Yulan Tang** received her Ph.D. degree from Jiangnan University, China. She is currently with Department of Robotic Control System, Wuxi Institute of Technology, China. Her current research include the layout and routing algorithm of FPGA.

**Jie Lv** received her M.S. degree from Shanghai University. She is currently with Department of Control Technology, Wuxi Institute of Technology, China. Her current research include electric transmission and power electronics applications.

**Yufang Zhang** received her Ph.D. degree from Harbin Engineering University. She is currently with Department of Robotic Control System, Wuxi Institute of Technology, China. Her current research include adaptive and nonlinear control in the field of industrial control.