Journal of Software Engineering

ISSN 1819-4311

Academic Journals Inc.

www.academicjournals.com

Journal of Software Engineering 9 (1): 50-65, 2015
ISSN 1819-4311 / DOI: 10.3923/jse.2015.50.65

A QoS-aware Trust Model for Multipath Load Balancing in Multimedia Sensor Networks

[1]Qian Ye, [2]Meng Wu and [3]Yufei Wang
[1]College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China
[2]College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China
[3]Research Institute of Information Technology and Communication, China Electric Power Research Institute, Nanjing, 210003, China

Corresponding Author: Qian Ye, College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China

ABSTRACT

QoS and security are two important factors which influence the application of the wireless multimedia sensor networks. Multipath routing is an effective approach to transmit large multimedia data in sensor networks to satisfy the QoS requirements. This study focuses on QoS-aware trust evaluation model and trust-based workload balancing among node-disjoint multiple routing paths created by multipath routing protocols. First, the trust level of single sensor node is calculated based on packet-drop rate, residual-energy and packet delivery queue length separately. Then, based on the trust value of single sensor node, the trust level of the single routing path is evaluated. Also the trust value fusion method for multiple routing paths is proposed. The overall grouping of routing paths increases monotonically, as the more trusted routing paths are added into the routing path group. Based on the proposed QoS-aware trust model, a load balancing algorithm among routing paths is designed. Finally, the proposed trust evaluation method and trust based load balancing algorithm are well analyzed and simulated. The analysis and simulation results show that our QoS-aware trust model can effectively evaluate the trust level of node-disjoint multiple routing path and affords a new secure and QoS-aware reference for designing multipath routing protocols.

Key words: Sensor networks, trust evaluation, multipath routing, trust fusion, workload balance

INTRODUCTION

Wireless Multimedia Sensor Networks (WMSNs) (Akyildiz *et al*., 2007), nodes of which equipped camera, mic and other sensors can produce multimedia information, are new advanced type of Wireless Sensor Networks (WSNs) (Akyildiz *et al*., 2002). Multimedia sensor nodes with the abilities of computing, storage and communication form distributed self-organizing sensing network. The WMSNs can sense, collect, process and transmit multimedia information such as audio, video, static image and scalar data in the field area they covered. As advanced type of WSNs, WMSNs have some same characters as WSNs: The strict abilities of sensor nodes and the network resource, large-scale, self-organized, multi-hop communication, dynamic topology, application related and data-center (Akyildiz *et al*., 2002). Meanwhile, WMSNs have its own distinct features (Akyildiz *et al*., 2007). The enhanced abilities of nodes and networks, rich types of multimedia information, complex processing task, comprehensive and effective sensing abilities.

The WMSNs applications, e.g., multimedia surveillance networks, target tracking, environmental monitoring and home automation systems require additional and new technologies to address the challenges for energy-efficient multimedia processing and communication in WMSNs, one of which is tight Quality of Service (QoS) requirements in terms of packet losses, delay and jitter (Akyildiz *et al*., 2007; Akan *et al*., 2008; Atzori *et al*., 2008). Differentiated-service like traffic scheduling and multipath routing are QoS approaches at network layer in WMSNs (Misra *et al*., 2008). Multipath routing is the common mechanism adopted for providing reliability in WSNs (Misra *et al*., 2008) and it is also considered an effective approach to transmit large multimedia data in WMSNs (Akyildiz *et al*., 2007).

QoS and security are two important factors which influence the application of the WMSNs. Cryptography based security solutions are usually not enough to protect WSNs from interior attacks caused by compromised nodes and trust management is considered effective to deal with this problem (Jing *et al*., 2008). The trust management has been widely researched in multi-agent systems (Han *et al*., 2013) mobile *ad hoc* networks (Govindan and Mohapatra, 2012) and sensor networks (Jing *et al*., 2008). Some trust-based multipath routing protocols have been designed for *ad hoc* networks. A Bayesian statistical model for a multipath trust-based reactive *ad hoc* routing protocol is proposed by Begriche and Labiod (2009). Trust-based on-demand multipath routing framework and protocol are given for mobile *ad hoc* networks by Li *et al*. (2010a), Qu *et al*. (2013) and Xia *et al*. (2013). The trust-enhanced anonymous on-demand routing protocol (TEAP) is proposed to restrain the misuse of anonymity (Gunasekaran and Premalatha, 2013). Also, lightweight trust management methods or frameworks for medical sensor networks are well studied (He *et al*., 2012). Li *et al*. (2013) designed a lightweight and dependable trust system for clustered wireless sensor networks. Feedback among cluster members is canceled and cluster header with richer resource is responsible for more computing and communication tasks (Li *et al*., 2013). For fault-tolerant data aggregation in wireless multimedia sensor networks, trust-based framework was designed by Sun *et al*. (2012). A trust-aware routing framework is designed, implemented to secure the WSNs against adversaries, misdirecting the multi-hop routing (Zhan *et al*., 2012). A highly scalable cluster-based hierarchical trust management protocol considering multidimensional trust attributes for WSNs is developed by Bao *et al*. (2012) to deal with selfish or malicious sensor nodes and the protocol is applied for trust-based routing and intrusion detection (Bao *et al*., 2012). However, 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.

This study establishes a trust computation model for node-disjoint multipath routing which includes trust evaluation of sensor node, single routing path and multiple routing paths and then a trust based load balancing algorithm was proposed among routing paths.

MATERIALS AND METHODS

Disjoint multipath routing in WMSNs: Clustering-based multi-tier topology is considered scalable network architecture for wireless multimedia sensor networks. Flat topologies may not be suitable for handling large amount of traffic in wireless multimedia sensor networks including audio and video (Akyildiz *et al*., 2007). We briefly introduce an example of a two layer hierarchy based on clustering in the following and then disjoint multipath routing is described using clustering-based two layer hierarchical topology.

In a clustering-based hierarchical network structure with multimedia sensor nodes organized into two layers, multimedia sensor nodes are grouped into clusters. Every cluster would have a

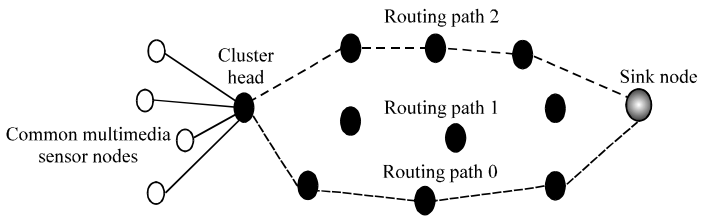

Fig. 1: Disjoint multipath routing in cluster based WMSNs

leader, often referred to as the cluster head. A cluster head multimedia sensor node may be richer in resources. All common multimedia sensor nodes belong to different clusters are joined to the lowest layer.

The multipath mechanism we consider, constructs a small number of alternate paths that are node-disjoint with each other. Disjoint multipath routing is used to establish multiple paths between each cluster-sink pair. Multimedia data generated by common multimedia sensor nodes are shipped to cluster head and then delivered to sink node through disjoint multiple paths which are assumed to be non-interfering. And non-interfering disjoint paths may be established if the number of paths is small. Figure 1 presents an example of disjoint multipath routing between one of cluster heads and sink node.

As shown in Fig. 1, three multiple paths do not share any common node nor any common link. We do not take into account about how to establish node-disjoint multiple paths. Trust evaluation methods proposed in this study is over multiple paths that have been established.

Description of QoS-aware trust evaluation problem: The model for the problem of trust level computation of multipath routing in wireless multimedia sensor networks is described here. The QoS assurance is an essential design factor of WMSNs. Due to the property of WMSN self-organization, limited resource, the QoS is hard to be guaranteed which greatly affects the network performance. The application-related QoS requirements reflect in aspects of multimedia data quality, network time-delay, network energy-consumption, coverage area and service time. Considering that trust is a crucial conception which can reflect the QoS among nodes, we propose the following solutions to quantify the trust value and select the trustable nodes for improving the service quality. We introduce three metrics to build the trust value of a node: time-delay, residual-energy and packet-drop-rate. These aforementioned factors we offered in the trust computing of sensor nodes because they are closely related to the behavior of the sensor nodes.

Let Q_1 represent packet-drop-rate, Q_2, represent residual-energy and Q_3 represent time-delay. We have the set of QoS requirements $Q = \{Q_1, Q_2, Q_3\}$.

For a deployed wireless multimedia sensor networks, let, V be the sensor nodes set. Multipath routing MR is designed for accomplishing multimedia data delivery from source node to destination sink node satisfying a set of QoS requirements Q. Multipath routing MR consists of $n \geq 1$ node-disjoint paths. To facilitate the present, let $MP^n = \{P_1, P_2, \ldots, P_n\}$ be the set of n node-disjoint paths between source node and destination sink node and routing path $P_i^{(k)} = (v_s, v_i^1, \cdots, v_i^k, v_d)$, in which, $v_i^m (1 \leq m \leq k) \in V$ denote the relay node in the i-th routing path ($P_i^{(k)}$), v_s is source node and v_d is the destination sink node. We segment the lifetime T of the established multiple routing paths into equal small time windows. Let:

$$T = \{\Delta t_1 \rightarrow \Delta t_2 \rightarrow \Delta t_3 \rightarrow ...\}$$

The trust values are computed at the end of the current time window and the trust value computed at the end of the time window Δt_r predicts the trust level in the next time window Δt_{r+1}.

For $1 \le i \le n$, let $0 < trust_{i,j}(\Delta t_r) < 1$ is the trust value of the QoS requirement Q_j based on i-th single routing path $P_i^{(k)}$ at the end of r-th time window Δt_r. Let $Trust_{\Gamma,j}(\Delta t_r)$ be the 'fused trust' of the QoS Requirement Q_j at the end of the r-th time window Δt_r based on a subset $\Gamma \in$(Power set of Mp^n) of routing paths. The 'fused trust' is the overall trust level of the QoS requirement based on a group of node-disjoint routing paths. The more satisfied QoS we obtain based on a routing path, the more trust we would have about it. At the end of r-th, time window Δt_r, the overall trust, $trust_{i,j}(\Delta t_r)$ of the i-th routing path $P_i^{(k)}$ was determined by fusing its individual trust $trust_{i,j}(\Delta t_r)$ for satisfying various QoS requirements. The overall trust, $Trust_{i,j}(\Delta t_r)$ of $\Gamma \in$(Power set of Mp^n) is determined by fusing individual trust, $trust_{i,j}(\Delta t_r)$ for satisfying various QoS requirements.

For $v_i^m (1 \le m \le k) \in V$ in the i-th routing path $P_i^{(k)}$, $0 \le trust_{(v_i^m,j)}(\Delta t_r) \le 1$ is the trust value of the QoS requirement Q_j at the end of r-th time window Δt_r. The overall trust, $trust_{v_i^m}(\Delta t_r)$ of node v_i^m is determined by fusing its individual trust, $trust_{(v_i^m,j)}(\Delta t)$ for satisfying multiple QoS requirements. At the end of r-th time window Δt_r, the objective is to:

- Determine the trust value $trust_{(v_i^m,j)}(\Delta t)$ and $trust_{(v_i^m)}(\Delta t)$ of sensor node v_i^m
- Determine the trust value $trust_{i,j}(\Delta t_r)$ and $trust_i(\Delta t_r)$ of the i-th routing path $P_i^{(k)}$
- Determine the trust value $Trust_{\Gamma,j}(\Delta t_r)$ and $Trust_\Gamma(\Delta t)$ of the routing path set $\Gamma \in$(Power set of Mp^n)

Methods of QoS-aware trust evaluation for multipath routing

Trust evaluation for sensor nodes: The trust level of the sensor node based on packet-drop-rate, residual-energy and the queue length of the sensor node separately is computed here:

- **Trust evaluation based on packet-drop-rate:** Motivated by the fact that monitoring the behavior of packet dropping will be helpful to identify the malicious or faulty nodes, we use the packet forwarding in the trust evaluation

For the sake of simplicity and to diminish the overhead in resource-constrained WMSNs, we applied only passive monitoring of forwarded packets to evaluate the trust value. In each time unit, the trust level based on packet forwarding is evaluated by the number of successful and unsuccessful packet delivery. The beta distribution has been proven useful for describing the probability distribution of binary events (Josang and Ismail, 2002).

First, for current time window Δt_r, we calculate packet delivery trust value $Ctrust_{(v_i^m,1)}(\Delta t_r)$ without packet delivery behaviors during history time windows. Let success_num(Δt_r) represent the number of successful packet delivery of node v_i^m and unsuccess_num(Δt_r) represent the number of unsuccessful packet delivery of node v_i^m during time window Δt_r. First, for current time window Δt_r, we calculate packet delivery trust value $Ctrust_{(v_i^m,1)}(\Delta t_r)$ without packet delivery rate during history time windows.

Let success_num(Δt_r) and unsuccess_num(Δt_r) be parameters used to describe beta distribution. $E(f(x; \alpha, \beta))$ is the estimated value of $Ctrust_{(v_i^m,1)}(\Delta t_r)$, where, α = unsuccess_num(Δt_r)+1, β = success_num(Δt_r)+1 and $E(f(x; \alpha, \beta))$ is the expected value of the probability distribution function of the beta distribution:

$$Ctrust_{(v_i^m,1)}(\Delta t_r) = E(f(x;\alpha,\beta)) \times \frac{1}{\sqrt{unsuccess\_num(\Delta t_r)+1}}$$

Where:

$$E(f(x;\alpha,\beta)) = \frac{\alpha}{\alpha+\beta} = \frac{success\_num(\Delta t_r)+1}{success\_mum(\Delta t_r)+unsuccess\_num(\Delta t_r)+2}$$

and:

$$\frac{1}{\sqrt{unsuccess\_num(\Delta t_r)+1}}$$

is strict punishment factor for unsuccessful packet delivery of sensor node, it will approach 0 rapidly with the increase of the number of unsuccessful packet delivery. Figure 2 shows the node trust values against successful and unsuccessful packet delivery without historical interactions.

The packet delivery trust values during history time windows should be taken into account in order to compute current trustworthiness. Supposing that sw history time windows is considered, that is the length of sliding window is sw, then the trust evaluation approach is defined by Eq. 1:

$$trust_{(v_i^m,1)}(\Delta t_r) = \begin{cases} \dfrac{\sum_{h=1}^{sw} f_h \times Ctrust_{(v_i^m,1)}(\Delta t_{r-h})}{\sum_{h=1}^{sw} f_h} & \text{when } r > sw \\ \dfrac{\sum_{h=1}^{r-1} f_h \times Ctrust_{(v_i^m,1)}(\Delta t_{r-h})}{\sum_{h=1}^{r-1} f_h} & \text{when } r \le sw \end{cases} \quad (1)$$

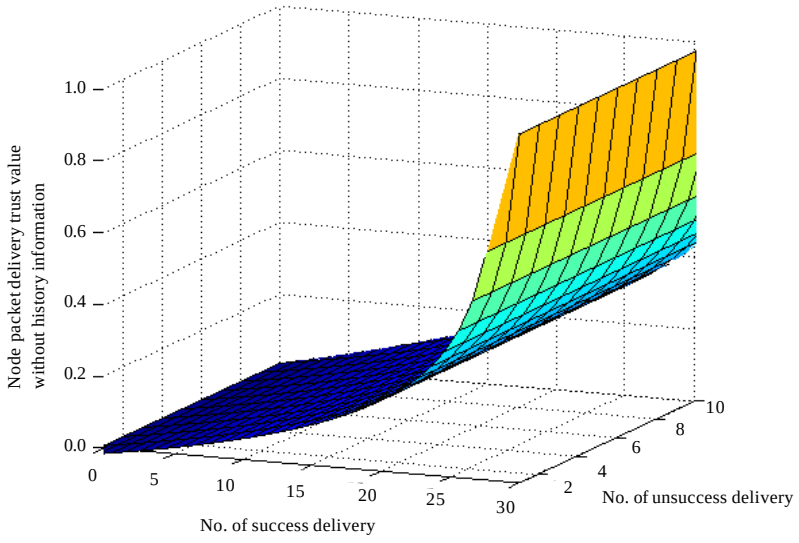

Fig. 2: Node packet delivery trust value of current time window without packet delivery rate during history time windows

The value $trust_{(v_i^m,1)}(\Delta t_r)$ calculated at the end of the time window Δt_r predicts the trust level in the next time window Δt_{r+1}.

We introduce decay function f_h ϕ^{sw-h}, $0<\phi<1$, $1 \le h \le sw$, $h \epsilon$ Integer to capture dynamic changes of node's behaviors. The exponential decrease method is used to deemphasize old historical behaviors. The coefficient ϕ represents the aging factor. A smaller f_h causes a greater decrease of decay function f_h and vice versa. More specifically, $f_1<f_2<...<f_h$ describes that the trust value made long time ago should carry less importance than the trust value made recently. The historical trust value made long time ago is not very useful for predicting node's future behavior.

- **Trust evaluation based on residual-energy:** Resource constraints are the biggest design challenges for WSNs. The energy, processing, memory and communication range of sensor nodes is very limited because of its low cost, small size and low power. So, residual-energy is a critical factor for evaluating the trust level of the senor node

Let, $RESIDUAL\_Er(v_i^m)$ represent the residual energy of sensor node v_i^m and $FULL\_Er(v_i^m)$ represent the initial full energy of sensor node v_i^m. Then the trust evaluation function is defined as follows:

$$trust_{(v_i^m,2)}(\Delta t_r) = \frac{RESIDUAL\_Er(v_i^m)}{FULL\_Er(v_i^m)} \quad (2)$$

- **Trust evaluation based on packet delivery queue length:** Time-delay is an important QoS consideration for WMSNs applications. The queuing time on relay sensor node is one of the critical factors influencing the time-delay of packet. The waiting delivery time of packets on the relay sensor node can be measured by the length of occupied buffer queues

We introduce $OCCUPY\_Len(v_i^m)$ to represent the length of the occupied receiving and sending buffer queues on relay node v_i^m and $BUFFER\_Len(v_i^m)$ to represent the full length of receiving and sending buffer queues on v_i^m. Evidently, the larger $OCCUPY\_Len(v_i^m)$ is, the longer time delay of packet delivery. The trust level based on packet delivery queue length can be denotes as follows:

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

Trust evaluation for single routing path: In general, routing path conditions include interference at intermediate hops, residual energy of the nodes and the number of backlogged flows along routing path, among others (Akyildiz *et al*., 2007). Accordingly, in our proposed scheme, the trust level of routing path conditions is evaluated by packet-delivery-rate, residual energy of nodes and time-delay of packet delivery.

For a single routing path $P_i^{(k)} = (v_s, v_i^1, \cdots, v_i^k, v_d)$, data is 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.

Considering the axiom (Sun *et al*., 2006) that concatenation propagation of trust does not increase trust and the opinion in information theory: The information cannot be increased via propagation (Xia *et al*., 2013; Mui *et al*., 2002), routing path trust value should not be more than the trust values of relay nodes (Li *et al*., 2010b).

- **Trust evaluation based on packet-drop-rate for single routing path:** Because the loss provability is multiplicative routing metric parameter (Wang and Crowcroft, 1996), the trust value of the packet-drop-rate based on routing path $P_i^{(k)}$ at time period Δt can be computed as:

$$trust_{i,1}(\Delta t_r) = \prod_{m=1}^{k}\left(trust_{(v_i^m,1)}(\Delta t_r)\right) \tag{4}$$

- **Trust evaluation based on residual-energy for single routing path:** Usually, energy cost is additive metric for routing path (Wang and Crowcroft, 1996). We argue that residual energy is concave for established routing path. For single routing path, once the energy of sensor node on routing path is exhausted, the routing path will be destroyed and invalid. And the new node must be selected to replace the energy exhausted relay node or new routing path must be established. Following the concave composition rule, the trust level of single routing path based on residual-energy can be defined as:

$$trust_{i,2}(\Delta t_r) = MIN[trust_{(v_i^1,2)}(\Delta t_r),\cdots,trust_{(v_i^k,2)}(\Delta t_r)] \tag{5}$$

- **Trust evaluation based on packet delivery queue length for single routing path:** It is obvious that time-delay follows the additive composition, so we can calculate the trust level of the single routing path based on packet delivery queue length as:

$$trust_{i,3}(\Delta t_r) = 1-\frac{\sum_{m=1}^{k} OCCUPY\_Len(v_i^m)}{\sum_{m=1}^{k} BUFFER\_Len(v_i^m)} \tag{6}$$

- **Trust fusion of single routing path:** For specific WMSNs application, the routing path might satisfy one or multiple QoS requirements. In order to evaluatE the comprehensive trust level of single routing path considering multiple QoS requirements, we fuse the trust value through the follow equations:

$$trust_i(\Delta t_r) = \eta_1 \times trust_{i,1}(\Delta t_r) + \eta_2 \times trust_{i,2}(\Delta t_r) + \eta_3 \times trust_{i,3}(\Delta t_r) \tag{7}$$

where, $0 \le \eta_1 \le 1$, $0 \le \eta_2 \le 1$, $0 \le \eta_3 \le 1$ and $\eta_1+\eta_2+\eta_3 = 1$. The value of η_1, η_2 and η_3 can be adjusted considering different QoS requirements of WMSNs applications

For a single routing path $P_i^{(k)} = (v_s, v_i^1, \cdots, v_i^k, v_d)$, Pseudo code of the trust evaluation algorithm for single routing path is given in Algorithm 1.

Algorithm 1: Trust evaluation algorithm for single routing path

Input: Single routing path $P_i^{(k)}$ between source node and destination node, η_1, η_2 and η_3

Output: $Trust_{i,1}(\Delta t_r)$, $trust_{i,2}(\Delta t_r)$, $trust_{i,3}(\Delta t_r)$, $trust_i(\Delta t_r)$

Set $trust_{i,1}(\Delta t_r) = 1$, $trust_{i,2}(\Delta t_r) = \infty$, $trust_{i,3}(\Delta t_r) = trust_i(\Delta t_r) = 0$

Set $OCCUPY\_Len(P_i) = BUFFER\_Len(P_i) = 0$

In time window Δt, destination node v_d sends message reversely to routing path $P_i^{(k)}$ to trigger the process of routing path trust value calculation

For each relay node $v_i^m \in P_i^{(k)}$ do

Compute $trust_{(v_i^m,1)}(\Delta t_r)$ using Eq. 1

Compute $trust_{(v_i^m,2)}(\Delta t_r)$ using Eq. 2

Compute length of occupied buffer $OCCUPY\_Len(v_i^m)$ on node v_i^m

$trust_{i,1}(\Delta t_r) = trust_{i,1}(\Delta t_r) \times trust_{(v_i^m,1)}(\Delta t_r)$

If $trust_{(v_i^m,2)}(\Delta t_r) < trust_{i,2}(\Delta t_r)$ then $trust_{i,2}(\Delta t_r) = trust_{(v_i^m,2)}(\Delta t_r)$ End if

$OCCUPY\_Len(P_i) = OCCUPY\_Len(P_i) + OCCUPY\_Len(v_i^m)$

$BUFFER\_Len(P_i) = BUFFER\_Len(P_i) + BUFFER\_Len(v_i^m)$

End for

$$trust_{i,3}(\Delta t_r) = 1 - \frac{OCCUPY\_Len(P_i)}{BUFFER\_Len(P_i)}$$

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

Return $trust_{i,1}(\Delta t_r)$, $trust_{i,2}(\Delta t_r)$, $trust_{i,3}(\Delta t_r)$ and $trust_i(\Delta t_r)$

- **Trust evaluation for multiple routing paths:** Before fusing the trust value of multiple routing paths, we make two assumptions. First, we assume that the trust value of routing path is more than 0.50. Second, the trust values of the multiple routing paths are mutually independent because the paths are node-disjoint. The overall trust value of a group of routing paths increases monotonically, as the more trusted routing paths are added into the routing path group

The trust fusion refers to the process of computing the overall trust value of a group of routing paths which have their own trust values. First, we compute the overall trust value of two node-disjoint routing paths. Given two routing path $P_i \epsilon MP^n$ and $P_1 \epsilon MP^n$ have their own trust value $trust_{i,j}(\Delta t_r)$ and $trust_{1,j}(\Delta t_r)$ for the QoS requirement Q_j at the end of time period Δt_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 Δt_r, in which $\Phi = \{P_i, P_1\}$, is computed as follows:

$$Trust_{\Phi,j}(\Delta t_r) = \frac{trust_{i,j}(\Delta t_r) \times trust_{1,j}(\Delta t_r)}{trust_{i,j}(\Delta t_r) \times trust_{1,j}(\Delta t_r) + \left(1 - trust_{i,j}(\Delta t_r)\right) \times \left(1 - trust_{1,j}(\Delta t_r)\right)} \quad (8)$$

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

$$Trust_{MP^i,j}(\Delta t_r) = \frac{Trust_{MP^{i-1},j}(\Delta t_r) \times trust_{i,j}(\Delta t_r)}{Trust_{MP^{i-1},j}(\Delta t_r) \times trust_{i,j}(\Delta t_r) + \left(1 - Trust_{MP^{i-1},j}(\Delta t_r)\right) \times \left(1 - trust_{i,j}(\Delta t_r)\right)} \quad (9)$$

Trust based load balancing algorithm among routing paths: In this section, we propose an algorithm for balancing loads among the trusted routing paths. Usually, we first compute the trust of routing paths from source node to sink node and then we select the routing path with the highest trust value. However, the routing path with the highest trust value will have immense workload while other capable routing paths with slightly lower trust value will have considerably less workload. The problem that will arise from this disproportionate allocation of workload is that the QoS will fall greatly due to the heavy workload present at the highly trusted routing paths. So, a load-balancing algorithm is required for sustaining good service quality in disjoint multipath routing.

In our trust based load-balancing algorithm, we first classify the multiple routing paths between source node and sink node into two groups, namely Good Trust Paths (GTP) and Bad Trust Paths (BTP) based on a threshold value of trust τ. Then we seek to choose a routing path from GTP by computing an approximate value of workload present at each routing path in GTP. Sorting the routing paths in GTP according to the increasing order of workload, the routing path with the smallest workload is selected. In the case of no routing path in GTP, we select a routing path from BTP based on trust value or randomly.

For routing path $P_i^{(k)} = (v_s, v_i^1, \cdots, v_i^k, v_d)$, we calculate an approximate value of workload $Load_{P_i}^{\Delta t}$ through the number of packets source node v_s has been sent to the first relay node v_i^1 in the routing path during the time window Δt. Workload $Load_{P_i}^{\Delta t}$ of routing path $P_i^{(k)}$ is computed using the following equations:

$$Load_{P_i}^{\Delta t} = Packet\_number^{\Delta t}(v_s \to v_i^1) \tag{10}$$

However, all the routing paths might be classified as bad trust paths in the initial stage of the system as their trust values might not have reached a stable state due to the lack of transactions. In such case, we choose a routing path based on the following probability:

$$Pro_{P_i}^{\Delta t} = \begin{cases} \dfrac{trust_i(\Delta t)}{\sum_{P_x \in BTP} trust_x(\Delta t)}, & \text{if } \sum_{P_x \in BTP} trust_x(\Delta t) \neq 0 \\ randomly\ \ choose, & \text{else.} \end{cases} \tag{11}$$

For multiple node-disjoint routing paths $MP^n = \{P_1, P_2, \ldots, P_n\}$ between source node and destination node, Pseudo code of the trust-based load balancing algorithm is given in Algorithm 2.

Algorithm 2: Trust-based load balancing algorithm

Input: Multiple node-disjoint routing paths Mp^n between source node and destination node

Output: Routing path P

For each $P_i \in MP^n$ do

Compute $trust_i(\Delta t)$ based on Algorithm 1

If $trust_i(\Delta t) \geq \tau$ then $GTP \leftarrow GTP \cup \{P_i\}$ Else $BTP \leftarrow BTP \cup \{P_i\}$ End if

End for

If $GTP \neq \Phi$ then

For each $P_i \in GTP$ do Compute workload $Load_{P_i}^{\Delta t}$ End for

Sort GTP in increasing order of workload

Return routing path P with the smallest workload

Algorithm 2: Continue

Else Compute $\sum_{P_x \in BTP} trust_x(\Delta t)$
If then $\sum_{P_x \in BTP} trust_x(\Delta t) > 0$
For each $P_i \in BTP$ do Compute $Pro_{P_i}^{\Delta t}$ End for
Return routing path P with probability $Pro_{P_i}^{\Delta t}$
Else
Return routing path P randomly
End if
End if

RESULTS AND DISCUSSION

The proposed trust computation model and load balancing algorithm was analyzed and simulated.

Trust computation model: The proposed trust evaluation method for sensor node based on packet-drop-rate considered the history information to compute current trustworthiness. Figure 3 shows node packet delivery trust value considering packet delivery rate during history time windows. We can see that, with historical trust, malicious sensor nodes cannot suddenly forget their past and start behaving well. That is, malicious sensor node cannot deceive others into believing that it is a trusted sensor by just behaving well in recent time window. A sensor node should perform normal for a number of time windows to gain confidence. Meanwhile, this also provides sensor node with opportunities to improve their trust values after a bad network traffic condition.

The trust of node-disjoint multipath routing is computed according to the overall confidence in a group of routing paths, where the individual routing path have their own confidence levels.

Figure 4 shows trust value fusion of three disjoint routing paths. Trust value of each routing path is more than 0.50. We can see that, assuming a routing path is trustworthy only if its trust value is more than 0.50: The fusion trust value of disjoint routing paths is higher than that of each routing path. Accordingly, multipath routing is more trustworthy than single routing path.

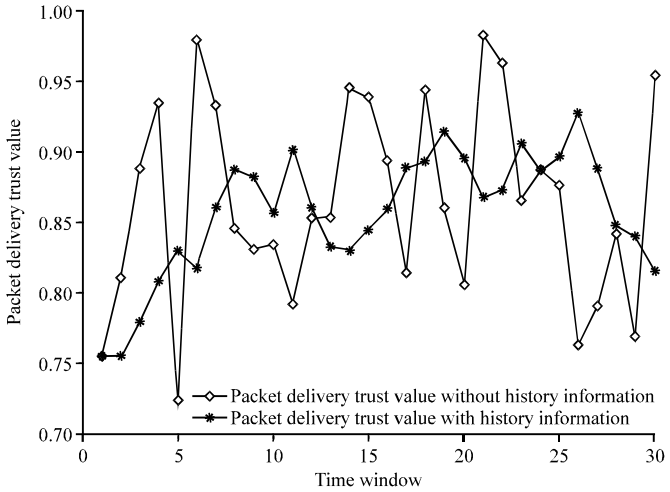

Fig. 3: Node packet delivery trust value considering packet delivery rate during history time windows (sliding window is 5)

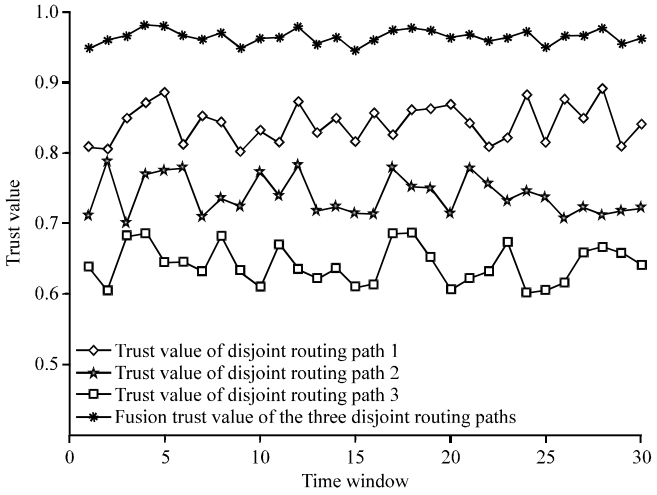

Fig. 4: Trust value fusion of three disjoint multiple routing paths (trust value of each routing path is more than 0.50)

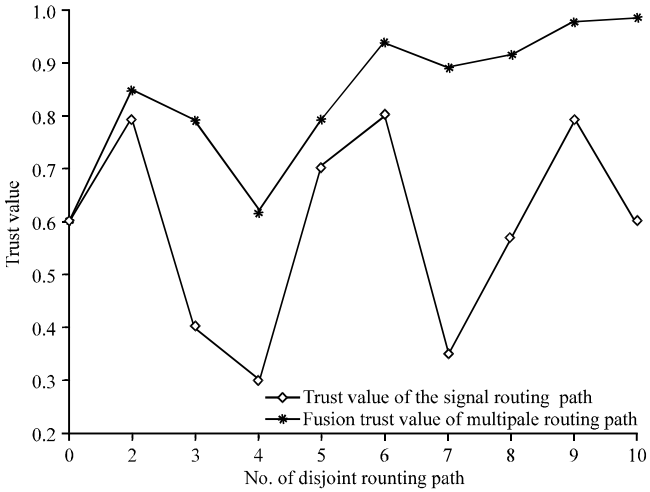

Fig. 5: Influence of the trust value of single routing path for overall trust value of multiple routing paths

For fusion trust value of multiple routing paths, Fig. 5 shows the influence of the trust value of single routing path. Given ten routing paths with different trust level, we calculate the fusion trust values with increasing the number of routing paths. We can see that, if the trust value of new routing path is less than 0.50, the overall trust value will decrease. Conversely, the overall trust value will increase if the trust value of new routing path is more than 0.50.

Trust based load balancing algorithm: In this study, we proposed an algorithm for balancing loads among the trusted routing paths. To analyze the validity of the proposed algorithm, we assume that there is only one coming packet during each time window.

Then Fig. 6 shows the load balancing process among 3 routing paths during 30 time windows and the load balance algorithm considers both the current trust level and current work load of each

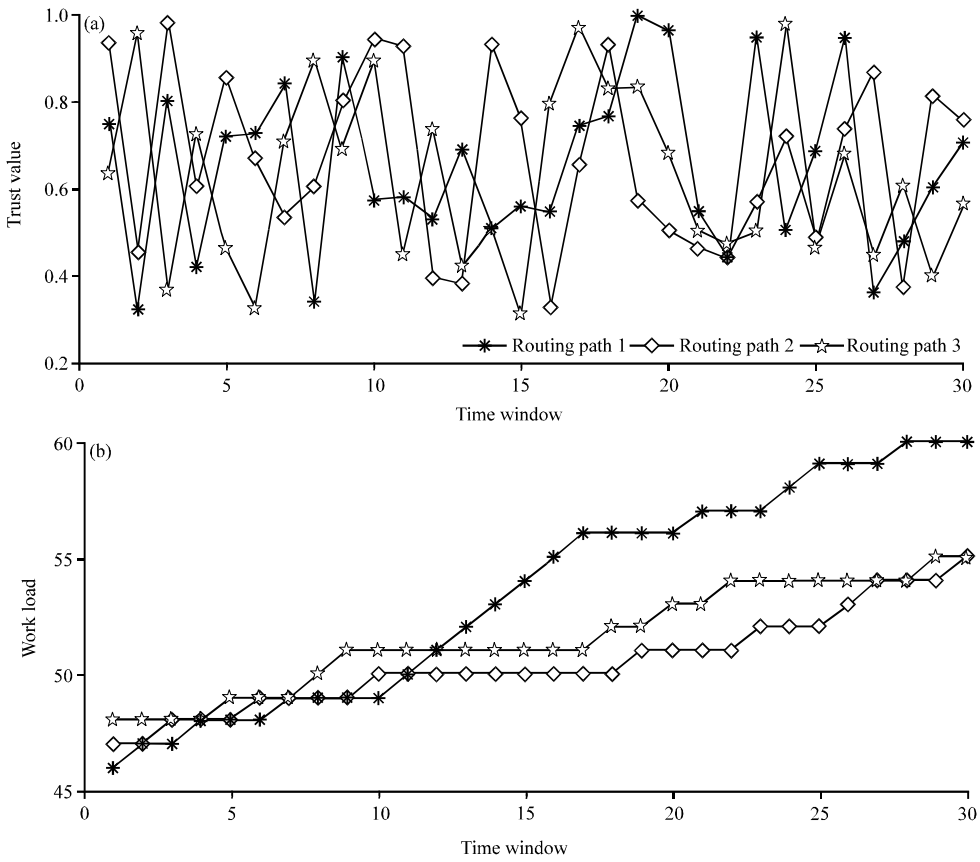

Fig. 6(a-b): Trust based load balancing among routing paths (threshold value is 0.7)

routing path. In Fig. 6, if the trust value of the routing path, work load of which is low, is less than the threshold value 0.7, then it will not be selected to deliver the coming packet. Among the routing paths, trust value of which are more than 0.7, the path with lowest work load will be selected to deliver the coming packet. If all the trust values are less than 0.7, then the routing path will be selected randomly to deliver the coming packet.

We simulate the proposed trust based load balancing algorithm in NS2 and the network topology was created as Fig. 1. The classic foreman_qcif.yuv, provided by TNK research institute was selected for test sequence, the format of which was 176×144 pixels. The test sequence was composed of 400 frames. The original frames were encoded to MPEG-4 and the format of the GOP (Group of Pictures) is IPBBPBBPIP.

Figure 7 show some frames of the simulation results. We can see that quality of the frames used, proposed trust based balancing algorithm is better than those using random balancing algorithm.

Figure 8 shows the PSNRs of the 400 frames. The PSNRs of the frames used proposed trust based balancing algorithm is higher than those using random balancing algorithm.

Comparison and discussion: We discuss the proposed QoS-based trust computation model in comparison to previously published trust evaluation methods for routing protocol, especially for multipath routing.

Fig. 7(a-c): Some frames of the simulation results of (a) Random packet delivery, (b) Packet delivery based on our proposed model and (c) Original frames

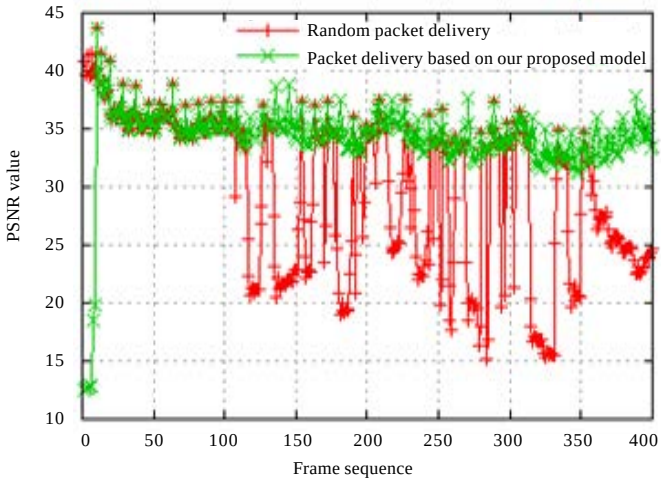

Fig. 8: PSNRs of the frames

Table 1: Comparison of different trust computing mechanisms used in routing protocol

Comparison	This study	Begriche and Labiod (2009)	Li *et al.* (2010a)	Qu *et al.* (2013)	Xia *et al.* (2013)	Zhan (2012)
Trust of nodes	√	√	√	√	√	√
Trust of single path	√	√	√	√	√	-
Trust of multiple paths	√	√	-	-	-	-
Considering packet delivery ratio	√	-	√	√	√	√
Considering energy	√	-	-	-	-	√
Considering queue length	√	-	-	-	-	-
Considering mobility	-	√	-	-	-	-
Using Bayesian method	√	√	-	-	-	-
Using proportion method	√	-	√	√	-	√
Using fuzzy logic rules	-	-	-	-	√	-
For routing in *ad hoc* networks	-	√	√	√	√	-
For routing in WMSNs/WSNs	√	-	-	-	-	√
For load balancing among routing paths	√	-	-	-	-	-

Based on the comparison as shown in Table 1, the key contributions and advantages of our proposed trust are:

- Developing a QoS aware trust computing model for disjoint multipath routing in WMSNs/WSNs, comprehensively considering packet-delivery-ratio, residual energy and queue length of sensor nodes
- Proposing a novel trust value fusion method for node-disjoint multiple routing paths, the fusion results can be used for evaluating the overall trust level of the established multiple routing paths (Fig. 4, 5)
- Based on the proposed trust model, designing a fresh load balancing algorithm for QoS-guaranteed multimedia transmission through multiple node-disjoint routing paths in WMSNs (Fig. 6-8)

CONCLUSION

In this study, we proposed a trust management model considering QoS factors for node-disjoint multipath routing in WMSNs. The proposed trust management framework included computation methods for sensor node, single path and multiple paths. Based on the proposed QoS-aware trust computation model, it was developed algorithms for trust-based load balancing. According to analyzing and simulating the algorithms, we concluded that our methods could afford an effective and secure QoS-aware reference for designing multipath routing and load balancing among multiple routing paths. In the years to come, we will focus on developing trust-based node-disjoint routing protocol suit for multimedia sensor networks.

ACKNOWLEDGMENT

This study is supported by the National Basic Research Program of China (2011CB302903), Scientific Innovation Research of College Graduate in Jiangsu Province of China (CX09B_152Z, CX10B_194Z), Key University Science Research Project of Jiangsu Province (10KJA510035) and Science and Technology Innovation Team Foundation for the "Qing Lan Project" in Jiangsu Province of China.

REFERENCES

Akan, O.B., P. Frossard, Q. Zhang and N. Jayant, 2008. Special issue on wireless multimedia sensor networks. Comput. Networks, 52: 2529-2531.

Akyildiz, I.F., T. Melodia and K.R. Chowdhury, 2007. A survey on wireless multimedia sensor networks. Comput. Networks, 51: 921-960.

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. A survey on sensor networks. IEEE Commun. Mag., 40: 102-114.

Atzori, L., T. Dagiuklas aned C. Politis, 2008. Special issue on multimedia over ad-hoc and sensor networks. Mob. Networks Applic., 13: 243-245.

Bao, F., I.R. Chen, M.J. Chang and J.H. Cho, 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Network Service Manage., 9: 169-183.

Begriche, Y. and H. Labiod, 2009. A bayesian statistical model for a multipath trust-based reactive ad hoc routing protocol. Proceedings of the 7th International Conference on Information, Communications and Signal Processing, December 8-10, 2009, Macau, pp: 1-8.

Govindan, K. and P. Mohapatra, 2012. Trust computations and trust dynamics in mobile *ad hoc* networks: A survey. Commun. Surv. Tutorials, 14: 279-298.

Gunasekaran, M. and K. Premalatha, 2013. TEAP: Trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks. IET Inform. Security, 7: 203-211.

Han, Y., S. Zhiqi, C. Leung, M. Chunyan and V.R. Lesser, 2013. A survey of multi-agent trust management systems. Access, 1: 35-50.

He, D., C. Chen, S. Chan, J. Bu and A.V. Vasilakos, 2012. ReTrust: Attack-resistant and lighweight trust management for medical sensor networks. IEEE Trans. Inform. Technol. Biomed., 16: 623-632.

Jing, Q., L.Y. Tang and Z. Chen, 2008. Trust management in wireless sensor netwroks. J. Software (China), 19: 1716-1730.

Josang, A. and R. Ismail, 2002. The beta reputation system. Proceedings of the 15th Bled Electronic Commerce Conference on e-Reality: Constructing the e-Economy, June 17-19, 2002, Bled, Slovenia, pp: 41-55.

Li, X., F. Zhou and J. Du, 2013. LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans. Inform. Forensics Security, 8: 924-935.

Li, X., Z. Jia, P. Zhang and H. Wang, 2010a. A trust-based multipath routing framework for mobile ad hoc networks. Proceedings of the 7th International Conference on Fuzzy Systems and Knowledge Discovery, August 10-12, 2010, Yantai, Shandong, pp: 773-777.

Li, X., Z. Jia, P. Zhang, R. Zhang and H. Wang, 2010b. Trust-based on-demand multipath routing in mobile ad hoc networks. IET Inform. Security, 4: 212-232.

Misra, S., M. Reisslein and G. Xue, 2008. A survey of multimedia streaming in wireless sensor networks. IEEE Commun. Surv. Tutorials, 10: 18-39.

Mui, L., M. Mohtsahemi and A. Halberstadt, 2002. A computational model of trust and reputation. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, January 7-10, 2002, Hawaii, USA., pp: 2431-2439.

Qu, C., L. Ju, Z. Jia, H. Xu and L. Zheng, 2013. Light-weight trust-based on-demand multipath routing protocol for mobile ad hoc networks. Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, July 16-18, 2013, Melbourne, VIC pp: 42-49.

Sun, Y., H. Luo and S.K. Das, 2012. A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks. IEEE Trans. Dependable Secure Comput., 9: 785-797.

Sun, Y.L., Y. Wei, H. Zhu and K.J.R. Liu, 2006. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE J. Selected Areas Commun., 24: 305-317.

Wang, Z. and J. Crowcroft, 1996. Quality-of-service routing for supporting multimedia applications. IEEE J. Selected Areas Commun., 14: 1228-1234.

Xia, H., Z. Jia, L. Ju, X. Li and E.H.M. Sha, 2013. Impact of trust model on on-demand multi-path routing in mobile ad hoc networks. Comput. Commun., 36: 1078-1093.

Zhan, G., W. Shi and J. Deng, 2012. Design and implementation of TARF: A trust-aware routing framework for WSNs. IEEE Trans. Dependable Secure Comput., 9: 184-197.