

Maximum-Objective-Trust Clustering Solution and Analysis in Mobile Ad Hoc Networks*

Qiang Zhang, Guangming Hu, and Zhenggu Gong

School of Computer, National University of Defense Technology,
Changsha 410073, Hunan, China
powerfbi007@sina.com, {gmhu, zhgong}@nudt.edu.cn

Abstract. In mobile-AdHoc networks (MANETs), many applications need the support of layer-structure. Clustering solution is the most widely used layer-structure and the choosing of clusterheads is the key problem of all. Traditional ways of clustering lack of instructions of trust mechanisms. This paper presents a maximum-objective-trust-based clustering solution (MOTBCS), which aims at the opinion of maximum stable links and energy viewpoint and gives nodes their objective trust estimation. This solution can be better suitable for the realistic working environments for MANETs. We make necessary simulations for our design and results show that MOTBCS can generate more stable clustering groups. It also has less communication costs and better efficiency than other clustering algorithms.

1 Introduction

Mobile ad hoc networks (MANETs) are self-organized wireless networks that are formed by mobile nodes through distributed protocols. MANETs can work without the support of communication infrastructure and such networks are being widely used in more and more fields. The features of dynamic topology and non-existence of central facilities ensure widespread application prospects of them, but at the same time these features bring about many new problems and challenges. Among them clustering of nodes is one of the biggest challenges that MANETs are facing with and it is also a hot spot in the research areas nowadays. Suited clustering solutions can greatly enhance the practicability and performance of MANETs[1].

Till now, researchers have raised a lot of clustering algorithms and some of them have been practically used, such as the Lowest-ID Algorithm[2,3], the Highest Connectivity Degree Algorithm[4], Distributed Clustering Algorithm(DCA)[5], Weighted Clustering Algorithm(WCA)[6,7] and k-hop Clustering Algorithm[8,9]. These algorithms each have different peculiarities and working environments.

* This research was supported by the National Grand Fundamental Research 973 Program of China under Grant No. 2003CB314802 and the National 863 Development Plan of China under Grant No. 2006AA01Z401.

2 Clustering

2.1 Definition of Clustering

MANETs nodes and links can be shown as an undirected graph $G(V,E)$. V denotes the set of nodes and E denotes the set of links. If there is a link $(u, v) \in E$, that means node u and v are 1-hop neighbors and they can communicate with each other directly. What we want to do is to choose a group of cluster-head nodes. They and their 1-hop nodes make up of the whole network.

Definition 1. The number of node V_i 's 1-hop neighbors is called V_i 's degree, and it is denoted by $D(V_i)$.

Definition 2. If there is a node $u \in V$ and u is in the range of V_i 's communication ability, and $(u, V_i) \in E$, then we called them neighbors. We use $N(V_i)$ to denote node V_i 's neighbor set, and $u \in N(V_i)$.

Definition 3. There are three node states in MANETs. They are pending nodes, member nodes and cluster-head nodes.

2.2 Stability of Clustering

In wireless networks, the signal intensity that nodes receive is tightly correlative with the distance between nodes. In the pure Friis free space model, $T_x P$ (signal sending power) and $R_x P$ (signal receiving power) have the following relation: (d is the distance between nodes)

$$\frac{R_x P}{T_x P} \propto \frac{1}{d^2}$$

While in actual environments, the expression $R_x P = \frac{c}{d^\alpha} T_x P$ is more accurate. But the value of α is not easy to set exactly.

Although it is not applicable to judge nodes' distance directly, we can estimate nodes' relative mobility with the consecutive message packets such as periodic "HELLO" packets. Assume that node u has received three periodic "HELLO" packets from node v , and the power is respective shown as $R_x P_{v \rightarrow u}^{(1)}$, $R_x P_{v \rightarrow u}^{(2)}$ and $R_x P_{v \rightarrow u}^{(3)}$, then we can define node v 's relative mobility degree as:

$$M_u^{rel}(v) = 10 \lg \frac{R_x P_{v \rightarrow u}^{(2)}}{R_x P_{v \rightarrow u}^{(1)}} + 10 \lg \frac{R_x P_{v \rightarrow u}^{(3)}}{R_x P_{v \rightarrow u}^{(2)}} \quad (1)$$

This way is somewhat like the definition of MOBIC[10]. If $R_x P_{v \rightarrow u}^{(2)} < R_x P_{v \rightarrow u}^{(1)}$, then $\lg \frac{R_x P_{v \rightarrow u}^{(2)}}{R_x P_{v \rightarrow u}^{(1)}} < 0$. That means node v is leaving away from node u . If $R_x P_{v \rightarrow u}^{(2)} > R_x P_{v \rightarrow u}^{(1)}$, then $\lg \frac{R_x P_{v \rightarrow u}^{(2)}}{R_x P_{v \rightarrow u}^{(1)}} > 0$. That means node v is moving towards node u .

Link Stability Estimation Rules

If node u and v meet the following demands, then we regard the link between them stable[13]:

1. The times that node u and v continuously send HELLO packets to each other equals or is more than 3;

2. If $M_u^{rel}(v) < 0$, then $|M_u^{rel}(v)| < M_{\min}^{Threshold}$;

3. If $M_u^{rel}(v) > 0$, then $M_u^{rel}(v) < M_{\max}^{Threshold}$

Here $M_{\min}^{Threshold}$ and $M_{\max}^{Threshold}$ are thresholds of relative mobility. Of course, $M_{\min}^{Threshold} < M_{\max}^{Threshold}$, and their actual values can be set according to the actual network environments.

3 Objective Trust

We mentioned the notion of node stability ahead, now we introduce the definition of objective trust.

Definition 4. Objective trust is more extensive than the notion of node stability. The decay of objective trust is a time-associated function[11]. We will combine it with the evaluation of node stability.

Definition 5. We mark the original objective trust with T_0 , and T_t after a period of time t .

Definition 6. $\theta(t)$ denotes the decay factor of objective trust. Then

$$T_t = \theta(t)T_0 \quad (t \geq 0) \quad (2)$$

Definition 7. We use λ to denote the ‘‘suspicion parameter’’ of objective trust.

Definition 8. Function of $f(t)$ can be denoted as:

$$f(t) = \begin{cases} \lambda e^{-\lambda t} & , \text{ when } t > 0 \\ 0 & , \text{ when } t \leq 0 \end{cases} \quad (3)$$

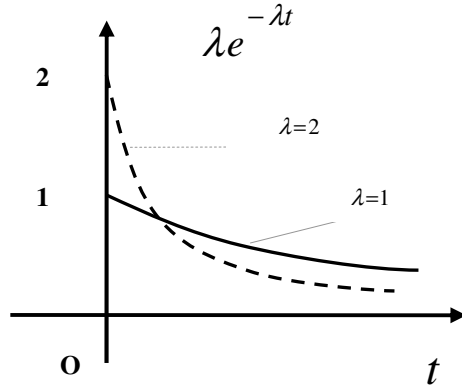


Fig. 1. Function of $f(t)$

Definition 9. We use $TSF(t)$ to denote the cumulation of decayed objective trust.

$$TSF(t) = \int_{-\infty}^t f(t') dt' = \begin{cases} 1 - e^{-\lambda t} & , t \geq 0 \\ 0 & , t < 0 \end{cases} \tag{4}$$

Then $\theta(t) = 1 - TSF(t)$

$$\theta(t) = e^{-\lambda t} \quad (t \geq 0) \tag{5}$$

The proofs of expression (3) and (5) are shown in Appendix I.

The objective trust and stability of nodes are relational with the ability of nodes in some degree, such as energy remains, computing speed and memory size. We use Cap_u to denote the integrative ability of node u . It is a discrete value after modifying.

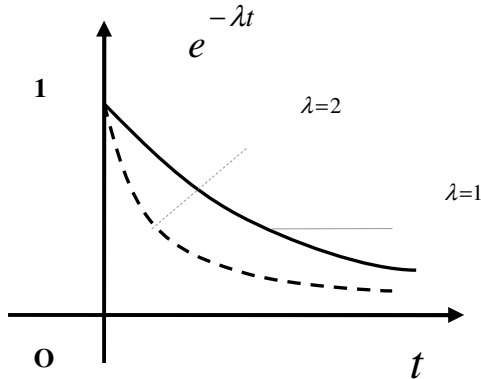


Fig. 2. Function of $\theta(t) = 1 - TSF(t)$

According to the upper objective trust model, the parameter λ_u can be set as follows. We first calculate the value of stable links N_u^{slink} and we set a quite big λ_{upper} beforehand.

$$\lambda_u = \begin{cases} \frac{1}{\sqrt{(N_u^{slink} \cdot Cap_u)}} & N_u^{slink} \neq 0 \\ \lambda_{upper} & N_u^{slink} = 0 \end{cases} \quad (6)$$

Assume that node u has k neighbors, and their relative mobility values to u are $M_u^{rel}(n_1)$, $M_u^{rel}(n_2)$, ..., $M_u^{rel}(n_k)$, then we define \overline{M}_u as node u 's integrative relative mobility.

$$\overline{M}_u = \sum_{i=1}^k \frac{|M_u^{rel}(n_i)|}{M} \quad (7)$$

In the upper formula, when $M_u^{rel}(n_i) < 0$, then M equals $M_{\min}^{Threshold}$; when $M_u^{rel}(n_i) \geq 0$, $M = M_{\max}^{Threshold}$. Of course, the less \overline{M}_u is, the more believable node u is.

4 Reconstruction of HELLO Message

The realization of MOTBCS is executed by reconstructing the message of HELLO. Since MANETs nodes send out HELLO packets periodically and they need brief computing, we can draw the following assumptions.

1. We can only consider λ (objective trust suspicion parameter) instead of complicated value of objective trust.
2. If no signal is received after a period of waiting time T_w (generally is twice larger than the cycle of HELLO packets), we can regard the link disabled referring to the tendency in Fig 2.

The new HELLO message with trust information can be shown as:

$$HELLO_i = (ID_i | Status | ntable | \overrightarrow{M}_i^{rel} | \overleftarrow{M}_i | Cap_i | timestamp | sk_i(hash))$$

Where ID_i : The ID number of node i ;

Status: This field has two choices of *ClusterID* and NULL. If it is NULL, that means the status of node is "Pending". If it is the ID of some node else, that means the node is node i 's clusterhead. If it is the ID number of node i itself, that means node i is a clusterhead.

ntable: the table of 1-hop neighbors to node i . Nodes can set up 2-hop topology by acquiring neighbors' 1-hop neighbors.

$\overrightarrow{M}_i^{rel}$: The relative mobility vector of node i . The components of $\overrightarrow{M}_i^{rel}$ can be stored in the table of *ntable*.

\overline{M}_i : Nodes' integrative relative mobility and it is computed from $\overrightarrow{M}_i^{rel}$

Cap_i : The integrative ability of node i , including its energy remains, computing speed and memory size. In this paper, we mainly concern nodes' energy.

timestamp: Current time.

$sk_i(\text{hash})$: The abstract information[12] to sign the message using the private key sk_i of node i .

We can divide the HELLO packets into three types for the difference of node *ID* and *Status* [13]:

Neighbor-search-message: its *Status*= NULL;

Clusterhead message: its *Status* = $ID_i \neq \text{NULL}$;

Cluster-join-message: its *Status* = $ID_j \neq \text{NULL}$ and $i \neq j$

Each node sets up a neighbor table and a 2-hop topology table. By using the table information and the periodic HELLO packages, we can work out the variables $\overrightarrow{M}_i^{rel}$, \overline{M}_i , N_i^{slink} and Cap_i . After that, the objective trust "suspicion parameter" λ_i can be computed, then the solution of MOTBCS showed below will select out the clusterhead of the group.

5 MOTBCS Algorithm

A pending node u (*Status* = NULL) chooses its clusterhead with the following algorithm MOTBCS.

ClusterHead(u)

IF (!initialized(G(V,E))) initialize(G(V,E))

IF (!assign(u .ID)) assign(ID) to u

IF (u .*Status* !=NULL) return ERROR;

$N'(u) = N(u) \cup \{u\}$ // $N(u)$: neighbor of node u

FOREACH node j ($j \in N'(u)$) **DO**

 compute $\overrightarrow{M}_i^{rel}$, \overline{M}_i , N_i^{slink} and λ_j ; // N_i^{slink} : number of stable links of i

ENDFOR

FOREACH neighbor node j ($j \in N'(u)$) **DO**

 select node with minimum λ_j ;

```

ENDFOR
IF nodes with minimum  $\lambda_j$  is only THEN
    node  $j$  becomes Clusterhead;
     $u.Status = j$ ;
    return;
ELSE
FOREACH node  $j$  with minimum  $\lambda_j$  DO
    select node with minimum  $\overline{M}_j$ ;
ENDFOR
IF node  $j$  with minimum  $\overline{M}_j$  is only THEN
    node  $j$  becomes Clusterhead;
     $u.Status = j$ ;
    return;
ELSE
FOREACH node  $k$  with minimum  $\overline{M}_k$  DO
    select node with minimum ID;
    node  $k$  with minimum ID becomes Clusterhead;
     $u.Status = k$ ;
ENDFOR
return;
ENDIF
ENDIF

```

6 Simulation and Experiments

We use network simulator ns-2 to do our experiments. Two widely used models are simulated in our tests. They are Random Waypoint Mobility Model(RWMM) and Reference Point Group Mobility model(RPGM). The behaviors and setting of the experiments are similar with that of [13].

6.1 Estimation Criteria

1. Clusterhead-Changing Frequency(CCF)

The status changing times of clusterheads in one second. A small CCF means a good clustering solution and a stable mobile adhoc network.

2. Node-Changing Frequency(NCF)

The status changing times of nodes in one second. A small NCF always means a stable mobile adhoc network.

3. Number of Clusterheads(NC)

The number of clusterheads changes when nodes move around in the network. Fewer clusterheads mean that a node can communicate with another node through fewer hops.

4. Communication Costs(CC)

The number of communication packages in one second. For simplification, we don't take the package encrypting into account.

6.2 Simulation Setting and Figures

We simulate the Lowest-ID Algorithm, Max-Degree Algorithm, Weighted Clustering Algorithm(WCA) and MOTBCS. The simulation parameters are shown in the following table.

Table1. Simulation Parameter Setting

Parameter	Description	Default Value
T_h	Cluster Message Cycle	2 s
T_w	Link Max-valid-time	4.2 s
T_c	Clusterhead Competing Interval	5s
Node number	Number of Mobile Nodes	60
Sim-time	Simulation time	600 s
Pause time	Pause Time When Moving in the Waypoint Model	4 s
Max-speed	Max Moving Speed	20 m/s
Tx-range	Range of Radio Transmission	30 to 180 m
Head-Energy-Use	Clusterhead Energy Use	0.03%/s
Member-Energy-Use	Normal Node Energy Use	0.01%/s
Length	Area Length	Sqrt (Num*3.14*150*150/8)
Width	Area Width	Sqrt (Num*3.14*150*150/8)

Simulation 1: Node-Changing-Frequency(NCF) vs. Communication Range(CR)

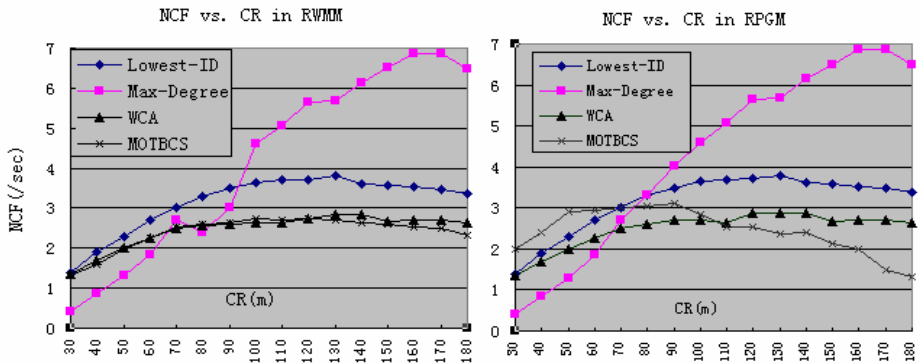


Fig. 3. NCF vs. CR

Simulation 2: Clusterhead-Changing-Frequency(CCF) vs. CR

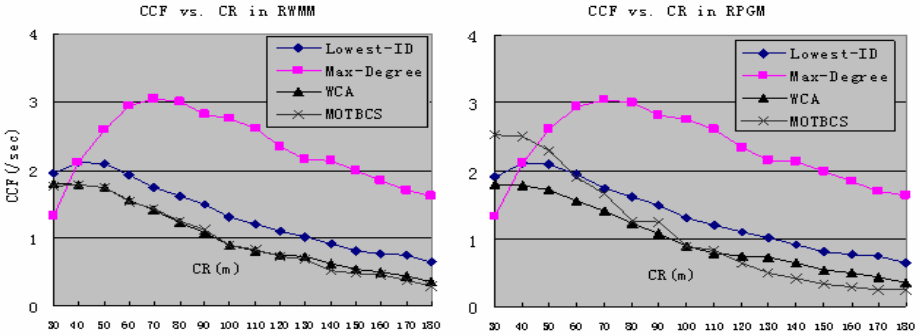


Fig. 4. CCF vs. CR

Simulation 3: Node-Changing-Frequency(NCF) vs. Node Speed(NS)

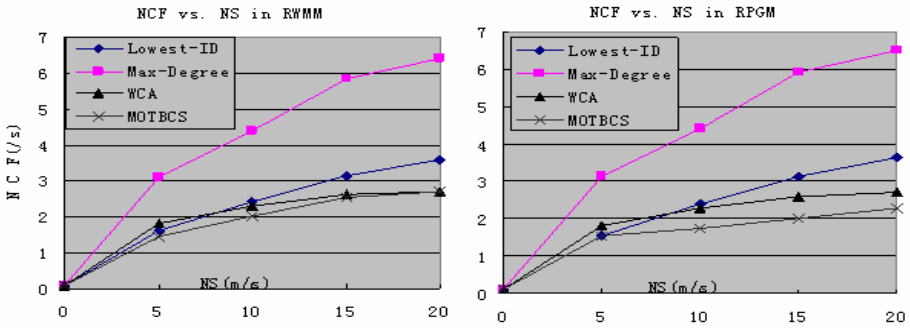


Fig. 5. NCF vs. NS

Simulation 4: Communication Costs(CC) vs. Communication Range(CR)

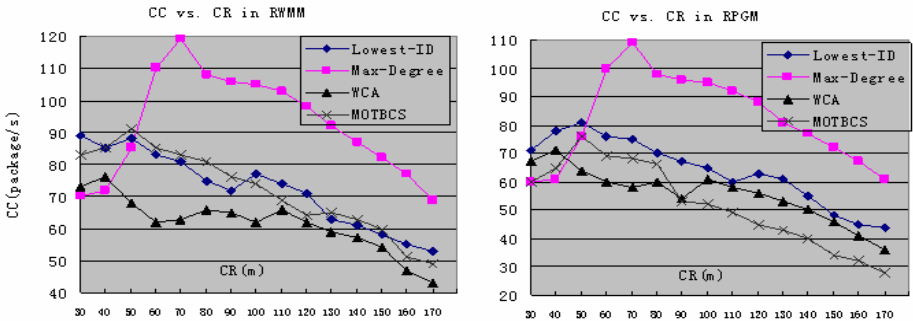


Fig. 6. CC vs. CR

Simulation 5: Communication Costs(CC) vs. Node Speed(NS)

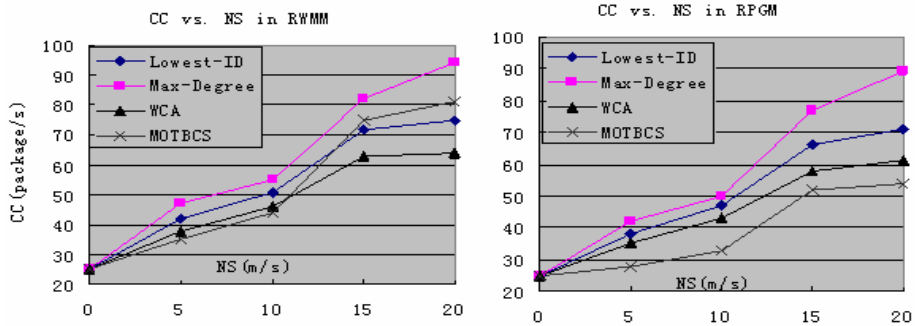


Fig. 7. CC vs. NS

Simulation 6: Number of Clusterheads in Experiments

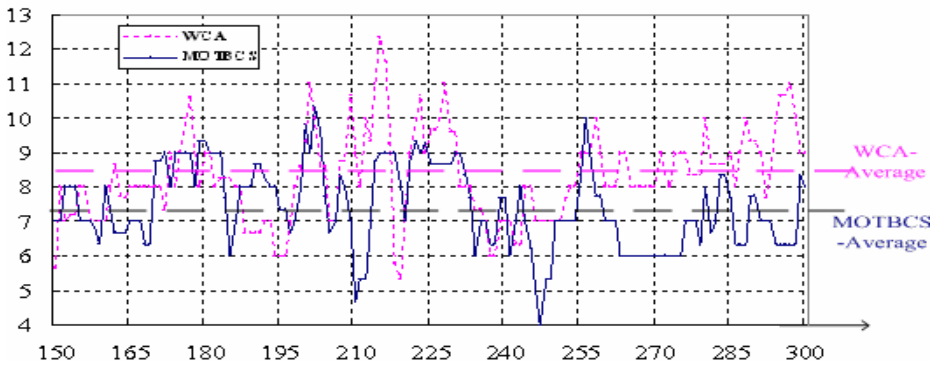


Fig. 8. Number of Clusterheads

6.3 Experiment Analysis

Fig.3 shows that NCF increases gradually when CR gets large. The reason is that when CR increases, the number of nodes in a cluster also increases. The performance of MOTBCS is better than the other three especially when $r > 100m$. That is because MOTBCS chooses the best objective trust nodes as clusterheads.

Fig.4 shows that when CR is about 50-70m, CCF is comparatively large. For at that time, the number of clusterheads is rather big and nodes are easy to compete to act as clusterheads.

We know from Fig.5 that NCF increases greatly when Node Speed gets large. But apparently, MOTBCS is more steady than the other solutions.

Fig.6 and Fig.7 compare MOTBCS's communication and control costs with the other three algorithms. Generally speaking, MOTBCS has better performance because

MOTBCS extends “HELLO” message to choose clusterheads instead of constructing new package, which reduces extra costs greatly.

Fig.8 shows that the average clusterhead number of MOTBCS is obviously less than that of WCA. That means nodes in MOTBCS need fewer hops to communicate with their copartners than in WCA.

7 Conclusion and Future Work

Mobile ad hoc networks (MANETs) are self-organized wireless networks that are formed by mobile nodes through distributed protocols. Clustering problem is one of the biggest challenges that MANETs are facing with and it is also one of the hottest spots in the research areas. This paper presents a maximum-objective-trust-based clustering solution(MOTBCS). It well takes into account objective trust and the relative mobility of nodes on the criteria for clusterhead selection. In this way, it overcomes the drawbacks of over-idealization assumptions about node behavior models in similar research, and thus is more applicable to realistic environments. Simulation results show that the MOTBCS solution can generate more stable clustering structure and has lower communication overheads, compared with other homologous algorithms. So MOTBCS can be a valuable solution for clustering with further realization in the future.

References

1. Varadharajan, V., Shankaran, R., Hitchens, M.: Security for Cluster Based Ad hoc Networks. *Computer Communications* 27(5), 488–501 (2004)
2. Ephrem ides, A., Wieselthier, J.E., Baker, D.J.: A design concept for reliable mobile radio networks with frequency hopping signaling[A]. *Proceedings of IEEE[C]* 75(1), 56–73 (1987)
3. Gerla, M., sai, T., Multiclust, J.T.C.: mobile, multimedia radio network [J]. *Wireless Networks* 1, 255–265 (1995)
4. Parekh, A.K.: Selecting Routers in Ad-Hoc Wireless Networks. In: *Proceeding of the SBT/IEEE International Tele. Symposium* (1994)
5. Basagni, S.: Distributed clustering for ad hoc networks[C]. In: *Proceedings of International Symposium on Parallel Architectures[C], Algorithms and Networks*, pp. 310–315 (1999)
6. Chatterjee, M., Das, S.K., Turgut, D.: WCA: a weighted clustering algorithm for mobile Ad Hoc networks [J]. *Journal of Cluster computing*, Special issue on Mobile Ad hoc Networking, 193–204 (2002)
7. Chatterjee, M., Das, S.K., Turgut, D.: An on-demand weighted clustering algorithm (WCA) for ad hoc networks[A]. In: *Proceedings of IEEE GLOBECOM 2000 [C]*, San Francisco, pp. 1697–1701. IEEE Computer Society Press, Los Alamitos (2000)
8. Krishna, P., Vaidya, N.H., Chatterjee, M., et al.: A cluster based approach for routing in Ad Hoc networks[J]. *ACM SIGCOMM Computer Communication Review (CCR)* (1997)
9. Amis, A.D., Prakash, R., Vuong, T.H., Huynh, D.T.: Max-M in D-Cluster formation in wireless Ad Hoc networks [C]. In: *Proceedings IEEE INFOCOM 2000*, Israel (2000)
10. Basu, P., Khan, N., Little, T D C.: Amobility based metric for clustering in mobile Ad Hoc networks [C]. In: *Proceedings of IEEE ICDCS 2001 Workshop on Wireless Networks and Mobile computing*, Phoenix, A Z, pp. 413–418. IEEE Computer Society Press, Los Alamitos (2001)

11. Zhang, Q., Li, D., Gong, Z., et al.: EDDTSTM: A Time-Nonlinear-Sensitive Trust Model Based on Human Mental Peculiarity in Virtual Computing Environments. Guangzhou, China. In: Proceeding of CIS. vol. 1, pp. 62–67 (2006)
12. Kuang, X.-H.: Research of Group Key Management in Mobile Ad hoc Networks. PhD thesis, National University of Defense Technology, Changsha, Hunan, P.R. China (2003)
13. Hu, G.-M.: Research on Key Security Issues in Clustered Mobile Ad hoc Networks. PhD thesis, National University of Defense Technology, Changsha, Hunan, P.R. China (2007)

Appendix I Proof of Expression (3) and (5)

Since λ is an objective trust suspicion constant, according to the mathematic fluxional way, we can conclude that:

$$\forall t > 0, \lim_{\Delta t \rightarrow 0} \frac{[T_{SF}(t + \Delta t) - T_{SF}(t)]|_{conditional}}{\Delta t} = \lambda$$

According to the conditional probability, the formula just equals to

$$\forall t > 0, \lim_{\Delta t \rightarrow 0} \frac{[T_{SF}(t + \Delta t) - T_{SF}(t)] / (1 - T_{SF}(t))}{\Delta t} = \lambda$$

Then we get the formula $T_{SF}'(t) / (1 - T_{SF}(t)) = \lambda$

So we can get $T_{SF}(t) = 1 - Ce^{-\lambda t} \quad (t \geq 0)$

We consider that $T_{SF}(t) = 0$ when $t \leq 0$, according to the formula $T_{SF}(0) = 0$, then we can know that $C = 1$, so we can conclude $T_{SF}(t) = 1 - e^{-\lambda t} \quad (t \geq 0)$. And as $f(t)$ is the probability density function of $T_{SF}(t)$, so formula(3) can be proved subsequently.

As $T_{SF}(t) = 1 - e^{-\lambda t} \quad (t \geq 0)$ is proved, and $\theta(t) = 1 - T_{SF}(t)$, so expression (5) of $\theta(t) = e^{-\lambda t} \quad (t \geq 0)$ is also proved.