A Trust Management Framework for Detecting Malicious and Selfish Behaviour in Ad-Hoc Wireless Networks Using Fuzzy Sets and Grey Theory

Ji Guo, Alan Marshall, Bosheng Zhou

Paper:
A Trust Management Framework for Detecting Malicious and Selfish Behaviour in Ad-Hoc Wireless Networks using Fuzzy Sets and Grey theory

J Guo, A Marshall, B Zhou

Preparation for Camera-Ready Contributions to LNCS/LNAI/LNBI Proceedings

The Institute of Electronics, Communications and Information Technology
Queens University Belfast, Belfast, UK
Belfast, United Kingom
{jguo04, a marshall, b.zhou}@qub.ac.uk

Abstract. As wireless network applications evolve, they require interaction between many entities (protocols, middleware etc), and an increasing requirement for the design of secure applications among the entities is trust management. Consequently, many new attacks against networks are aimed at the trust management. In this paper, we develop a new trust management framework (TMF) for wireless networks. The proposed framework applies Grey theory combined with Fuzzy Sets to calculate a node's trust value based on observations from neighbour nodes'. The new TMF employs multiple rather than a single parameter to decide the resulting trust value. Simulations conducted in an 802.11 based wireless network show that the new framework can not only identify abnormal trust behaviour, but can also effectively find which aspect of the metrics used to establish the trust value for a node are abnormal, and hence identify the strategy the attacker is using against the TMF.

Keywords: trust management framework, Fuzzy Set, Grey theory, wireless networks.

1 Introduction

Wireless network technologies have greatly changed our daily lives by offering access to the Internet anywhere and anytime. However attacks and intrusions against wireless networks, Internet fraud and high-tech crimes have kept raising in recent years, and security has become a major concern for those who intend to use wireless technologies and Internet services. Substantial resources have been deployed to tackle this issue; firewalls, anti-virus software, encryption algorithms, and intrusion

detection and prevention systems are examples of the tools to secure network applications. A networked application involves interactions among many entities, such as networking protocols from physical layer to application layer, middleware, various algorithms, etc. An essential challenge when designing a secure application is therefore to determine how one network entity can trust another network entity.

In today's business communications systems, trust plays an important role in virtual organizations, where it is used to counter uncertainty caused by the business requirement for openness. The requirement seeks to make marketable services openly available to all potential, highly autonomous clients, which increases a service provider's vulnerability to an attack [1]. Especially in distributed environments, trust management can provide a basis for more detailed and better-informed authorization decisions, while allowing for a high level of automation. Researchers want to design trust management systems in order to establish trust relationships, dynamically monitor, and adjust any existing trust relationships [1][2]. In recent years, various models and algorithms for describing trust and designing trust management in distributed systems or wireless networks have been considered, such as policy language, public-key cryptography, the resurrecting duckling model, and the distributed trust model [1][2][3][4]. The distributed trust models are usually applied in peer-to-peer (P2P) systems and wireless ad hoc Networks; these networks rely on all participants actively contributing to network activities such as routing and packet forwarding. The particular characteristics of a wireless network's nodes, such as limited memory, battery power, and bandwidth, can provide incentives for them to act selfishly (refuse to participate in routing and provide services to other nodes, for example). Trust management can help mitigate nodes' selfish behaviors and advantage the efficient utilization of network resources. Recent research has considered how to evaluate the trust of communication entities in wireless networks, and various theories such as Probabilistic Estimation [1], Information Theory [4], Fuzzy theory, and Game theory have been used for designing the trust metrics [5][6]. For evaluating trust values from more aspects, some researchers introduce Grey theory to improve existing trust management or network performance [7][8][9][10].

In this article, we focus on designing a new trust management framework which uses algorithms based on Fuzzy Sets and Grey theory. Grey theory has been widely applied in many fields like economics, agriculture, aerographs, the environment and materials. In [7][9], Deng Julong proposed the grey relational analysis method to make a quantitative analysis of the dynamic development process of systems. The basic idea of Grey theory is to determine the relationship of different factors according to the degree of similarity between curves. The research presented here takes the idea of Grey theory in order to rank trust values. A major advantage of this method is that it does not require a high quantity of sample data. Moreover, it does not require the data to be consistent with any kind of distribution rule in order to produce very convincing results, which are consistent with qualitative analysis. In [8], Fu Cal *et al* applied an improved traditional analysis method to the problems mentioned above. This method can effectively deal with data that has multiple attributes, while obtaining grey relational grades that can be compared with each other, no matter what the units of the original data are [8]. It can therefore be considered a feasible method for risk assessment of peer nodes in P2P networks and wireless ad-hoc networks.

The rest of this article is organized as follows: first, the classification of trust relationships is introduced, then the application of Grey theory to the design of a new trust management framework is described. Several simulation cases are then described that use the proposed algorithms and their performance examined. Conclusions and further research are then detailed.

2 Trust relationships

Current trust management research in wireless networks, usually views the neighbourhood from three levels [1][4][11]. For the neighbourhood of one node, according to the link conditions, we can classify as direct, indirect, and recommendation relationships, on behalf of node A's different neighbours' trust opinions.

Direct trust is established through observations on whether the previous interactions between the nodes have been successful [11]. For example, node A wants to know node B's information, for which observations from A to B are for direct trust.

Indirect trust can be transited through the third entities. For example, node *E* and *F* are the indirect trust nodes, which have interactions with *B*, but not with *A*.

Recommendation trust is a special type of trust relationships. We assume the nodes have a common node to communicate. This common node is denoted as the recommendation node. For example, nodes *A* and *B* have a common node *C*. If *A* wants to know the trust records of *B* from *C, C* will calculate the trust value of *B* based on the observations of interactions between *B and C*.

3 A new Trust Management Framework for Wireless Networks using Fuzzy Set and Grey Theory

This section presents a TMF for a pure mobile ad hoc network environment, using Grey Theory. The TMF is designed to be robust against attacks that are aimed to deceive the trust relationships, such as Selective Misbehaviour attack, On-off attack, Conflicting attack, and Bad Mouthing attack [1][11]. In wireless ad-hoc and mesh, the links between communicating nodes can be one-hop, and multi-hop, only single-hop links are considered in this paper.

3.1 The framework

For a node in a distributed environment, such as in a wireless ad hoc network, the trust management of the network views the node as an agent for obtaining the trust information. The functional blocks of the framework are shown in Figure 1.

In Figure 1, the nodes in the TMF firstly collect the input information for subsequent computation of trust. Many existing trust models for distributed environments choose the probability of successful interactions, which is generally viewed as corresponding to the packet loss rate, as the main parameter in calculation of the trust value. However, in fact the probability of one node cooperating with other nodes is influenced not only by the packet loss rate, but also signal strength, data rate, and other physical factors that are not considered in current trust models.

For example, an attacker/selfish node may make use of the knowledge that the packet loss rate is the main parameter used in trust calculation. Due to this limitation,

the attacker can obtain a very high trust value by just interacting with close neighbours, while dropping or abandoning communications with nodes far away. In comparison, normal behaving nodes will communicate with *all* neighbours (near and far). However when a normal node interacts with a far away neighbour, the packet loss rate may be higher than that of the attacker which communicates only with near neighbours. Thus, if only the packet loss rate is used as the deciding parameter, it will lead to a normal node's trust value being lower than the attacker's who intends to choose partners. This leads to the conclusion that any TMF should consider multiple parameters, including those involved in the communications processes in order to avoid such duplicity.

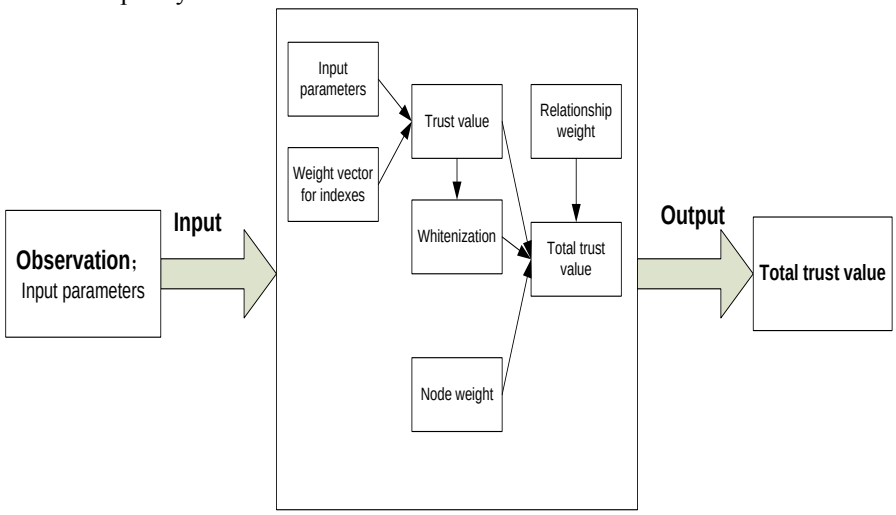


Figure 1 - functional blocks of the TMF

The input parameters include: packet loss rate, signal strength, data rate, end-to-end delay, and throughput. These parameters are chosen as the basic minimum set of parameters required to cover all types of attacks against lower level protocols as they can easily be obtained from MAC, data link and network layer protocols.

3.2 Using Grey Theory

For multiple input parameters, we can use Grey Theory to proceed and calculate trust value. From Grey theory, let X be a grey relational set which is used as the evaluation index set, $X = \{ x_1, ..., x_m \}$, while x_j is an evaluation index. Here, we assume that $X=\{$*packet loss rate, signal strength, data rate, delay, throughput*$\}$.

During a time period t $(t=1,2,...T)$, from the view of a node that observes its neighbouring node k's behaviour and calculates its trust values, k's value of the evaluated index x_j is $a_{kj}^{\ t}$ $(j=1,2,...,m)$. We can get node k's sample sequence $A_k^t = \{a_{kj}^t\}$, $j=1,2,...,m$, and the sample matrix for all the neighbouring nodes at t, $A^t = [a_{kj}^t]$, $j=1,2,...,m$, $k=1, 2,..., K$.

We define at period t, the best reference sequence $G^t=(g_1^t,..., g_m^t)$, while g_j^t is the chosen best index from $\{a_{kj}^t\}$. From Grey theory, we can obtain the Grey Relational Coefficient [6] between node k's sample and the best reference sequence about x_j at period t as:

$$\theta_{k,j}^{\ t} = \frac{\min_k \left|\alpha_{k,j}^{\ t} - g_j^{\ t}\right| + \rho \max_k \left|\alpha_{k,j}^{\ t} - g_j^{\ t}\right|}{\left|\alpha_{k,j}^{\ t} - g_j^{\ t}\right| + \rho \max_k \left|\alpha_{k,j}^{\ t} - g_j^{\ t}\right|} \quad ...(1)$$

$\rho \in (0,1)$ is the distinguishing coefficient [8]. Also we define the worst reference sequence $B^t=(b_1^t,..., b_m^t)$, while b_j^t *is* the chosen worst index from $\{a_{kj}^t\}$. From Grey theory, we can obtain the Grey Relational Coefficient between node k's samples and worst reference sequence about x_j at period t as:

$$\phi_{k,j}^{\ t} = \frac{\min_k \left|\alpha_{k,j}^{\ t} - b_j^{\ t}\right| + \rho \max_k \left|\alpha_{k,j}^{\ t} - b_j^{\ t}\right|}{\left|\alpha_{k,j}^{\ t} - b_j^{\ t}\right| + \rho \max_k \left|\alpha_{k,j}^{\ t} - b_j^{\ t}\right|} \quad ...(2)$$

$\rho \in (0,1)$ is distinguishing coefficient. From *(1)* and *(2),* when normally setting $\rho=1/2$, the value area of a grey relational coefficient is from *0.33* to *1*. In order to make the grey relational coefficient to be in *[0, 1],* it can convert the values by using the mapping $y=1.5x-0.5$ (x is the grey relational coefficient*)*.

We define the index set X's weight vector $H=\{h_1,..., h_m\}$, $\sum h_j=1$. At period t, node k*'s* Grey Relational Grades with best and worst reference sequence are $\theta_k^{\ t} = \sum_j h_j \theta_{k,j}^{\ t}, \phi_k^{\ t} = \sum_j h_j \phi_{k,j}^{\ t}$, respectively.

Then, by using the least-square methods [12], we can obtain the integrated expected value at period t as node k's trust value:

$$T_k^{\ t} = \frac{1}{1 + \frac{(\phi_k^{\ t})^2}{(\theta_k^{\ t})^2}} \quad ...(3)$$

3.3 Overall Trust Value with Fuzzy Set and Whitenization Weight Function

The trust models currently used seldom consider the influence of different nodes' viewings; moreover, they also set the weights of the opinions as fixed values, usually average values. This means the important degrees of opinions about trust information from a normal node and a selfish node (or an attacker) are equal. Therefore, our approach is to set the weights as changeable parameters in order to express the degree of trust of a node or nodes, based on their historical behaviour.

We can obtain the trust assessment by using classes of grey clusters and a whitenization weight function. Grey whitenization weight function can be used to measure the utility value of expected revenue [9][13]. This means that whitenization weight functions can describe one value's weights in different clusters, which can be viewed as the degree of how much the value belongs to a cluster. We define n grey clusters $c_1, c_2, ..., c_n$ for evaluating trust degrees, the corresponding whitening functions $f_1(x), f_2(x), ..., f_n(x)$, and the threshold values $\sigma_1, \sigma_2, ..., \sigma_n$ [7]. Three classes of grey clusters are defined as shown in table 1.

Table 1 - Grey clusters

c_1	Not quite trusted
c_2	Some trust
c_3	Quite trusted

The corresponding whitenization functions are as follows:

$$f_1(x)=\begin{cases}1, x<=0.25\\ -4x/3+4/3, x>0.25\end{cases},\ \sigma_1=0.25 \qquad ...(4)$$

$$f_2(x)=\begin{cases}2x, x<=0.5\\ -2x+2, x>0.5\end{cases},\ \sigma_2=0.5 \qquad ...(5)$$

$$f_3(x)=\begin{cases}4x/3, x<=0.75\\ 1, x>0.75\end{cases},\ \sigma_3=0.75 \qquad ...(6)$$

When node A gets various trust values of node B from different neighbor nodes. The whitenization weight of a trust value T_{Bk} (node *B*'s trust value evaluated by node *k,* also named as T_k) belonging to the *j* class c_j is $f_j(T_{Bk})$. According to $max_j\{f_j(T_{Bk})\}$, we can know the grey cluster class of *node B* based on T_{Bk}.

$$T_{total}=\frac{1}{2}(\max_j\{f_j(T_{direct})\})T_{direct}+\frac{1}{2}\frac{2N_R}{2N_R+N_I}\sum_k\frac{w_k}{\sum w_k}(\max_j\{f_j(T_k)\})T_k$$
$$+\frac{1}{2}\frac{N_I}{2N_R+N_I}\sum_k\frac{w_k}{\sum w_k}(\max_j\{f_j(T_k)\})T_k \qquad ...(7)$$

Here, $\rho=1/2$; *Nr* means the number of recommendation nodes, while *Ni* means the number of indirect nodes. The *Nr* and *Ni* can express the effect levels of different trust relationships, to compose relationship weights. w_k (or w_{kA}) is the weight value of node *k* that is set by node *A*. From $max_j\{f_j(T_{total})\}$, it can get the total grey cluster class for *node B*.

4 Simulation and analysis

The experiment scenario used ns-2 to create a wireless environment, using 802.11 standards, to simulate 6 wireless nodes in a distributed MANETs like structure shown in Figure 2. *node 0* wants to get the trust value of *node 1* based on trust opinions from *node 0* and its neighbouring nodes *2, 3, 4 & 5*.The DSDV routing protocol is used.

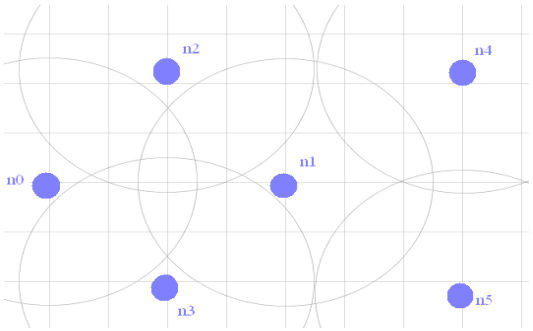


Figure 2 Topology of the 6 wireless nodes

4.1 Direct and Recommendation trust values

In this part, the simulation sets 6 nodes and calculates 4 nodes' trust values from them. All the nodes are static. Each link from node *i* to node *j* has a 10-second

CBR/UDP traffic. The size of each data packets is 220 Bytes. The parameters observed are: packet loss rate; received signal strength; delay; throughput; data rate (currently set as a fixed value 1.0Mbps, 802.11 basic data rate). Initially all parameters have equal importance (equal weight).

From Grey Theory, we can use the input parameters of a node to calculate the target node's (*node 1)* trust value, from the view of a specified node like *node 0*, compared with the neighbour nodes of *node 0*. That means by Grey Theory, we get *node 1*'s trust value from *node 0*, which has neighbouring nodes *node 2 and node 3*. The TMF gets the three nodes' (*node 1, 2, 3*) trust values for *node 0* over a period of 10 seconds, which is $T_{10}=0.44509$ as the direct trust value of *node 1*. Here $\rho=0.5$, $H=\{0.2,0.2,0.2,0.2,0.2\}$, $N_R=2$, $N_I=0$, which means the indirect nodes *4, 5* are not included. All the initial weight values w_{k0} are set to 1.

The framework also gets $T_{12}=0.22490$, *and* $T_{13}=0.20000$, which are the recommendation values from nodes *2* and *3* about node 1. After the whitenization functions, the total value of *node 1* for *node 0* with 3 neighbor nodes is $T_{10\text{-}3nodes}=0.30433$, as shown in Figure 3.

4.2 Direct, Recommendation and Indirect trust values

Here, the system calculates the trust values among 6 nodes, considering several additional links. $\rho=0.5$, $H=\{0.2,0.2,0.2,0.2,0.2\}$, $w_{k0}=1$, $N_R=2$, *and* $N_I=2$.

From the simulating data, we get $T_{10}=0.44509$, *and* $T_{12}=0.22490$, $T_{13}=0.20000$, $T_{14}=0.80000$, and $T_{15}=0.50000$. From these it is possible to calculate the total trust value with 5 neighbor nodes $T_{10\text{-}5nodes}=0.37726$, as shown in Figure 3. From $max_j\{f_j(T_{10\text{-}5nodes})\}$, we can know *node 1*'s grey cluster class is c_1.

4.3 Analysis

In Figure 3, there are the trust values of node 1 from node 0, 2, 3, 4, 5, and the total values with 3 nodes and 5 nodes, the average value $T_{10\text{-}average}$ of T_{10}~T_{15}.

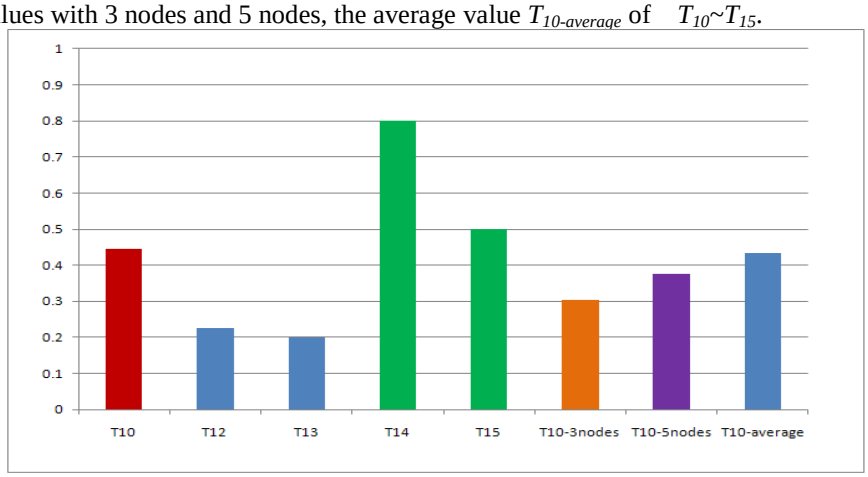


Figure 3 trust values

From the figure, the results show that taking different relationship factors will affect the total value. $T_{10\text{-}average}$ is higher than $T_{10\text{-}3nodes}$ and $T_{10\text{-}5nodes}$, due to not including the relationship weights. If the simulation just considers the opinions of

nodes *0, 2, 3*, the result will be lower than that including nodes *0, 2, 3, 4, 5* because T_{15} is higher than T_{13}, and T_{14} is higher than T_{12}.

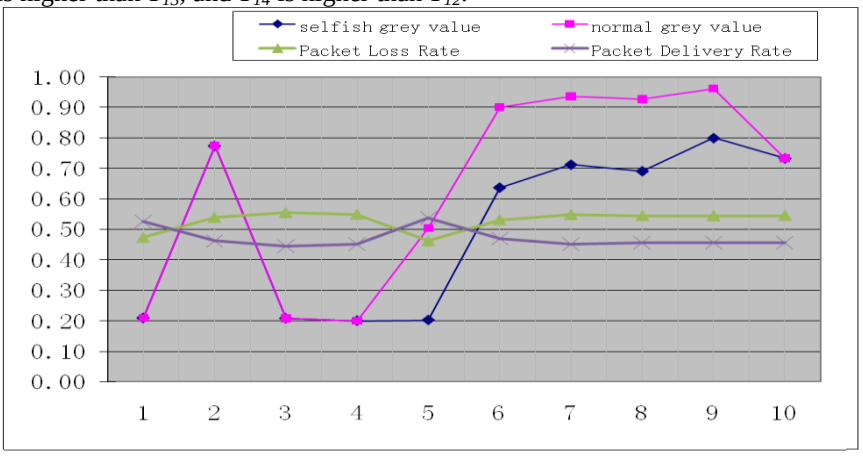
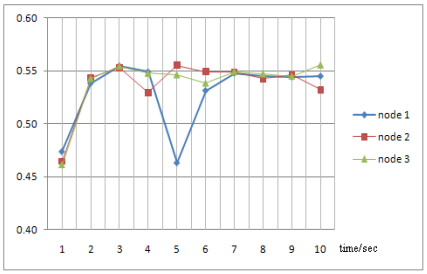
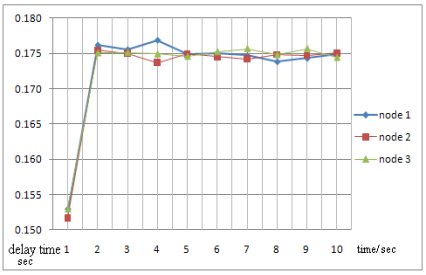


Figure 4 - Trust values calculated by grey theory and PDR

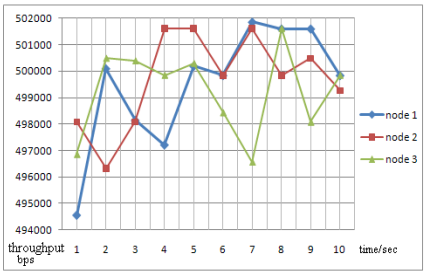
Figure 4 shows the trust values calculated by grey theory, and PLR (Packet Loss Rate) which is often the single metric selected by current TMF approaches such as OTMF (Objective Trust Management Framework) [1]. Existing trust management schemes like OTMF, often choose the probability of successful interactions as their input parameter in order to calculate their trust values.



(a) PLRs of node 1, 2, 3



(b) Delays of node 1, 2, 3



(c) Throughputs of node

Figure 5 – Trust Parameters of nodes *1, 2, 3* for 10 seconds

For nodes *0, 1*, the simulation takes a 10-second CBR/UDP traffic from *node 0* to *node 1*. Every second as an interval, the simulator calculates and records the grey trust value of *node 1* from *node 0*, compared with the good-put trust values obtained

from the packet delivery rate (PDR) of *node 1*. The good-put trust value obtained from the packet delivery rate is equal to *1-PLR* . T_{10} in Figure 3 is the grey trust value of *node 1* from *node 0* for the period of 10 seconds, while the good-put trust value of *node 1* for the period of 10 seconds is 0.463517. The result clearly shows that the individual good-put sample values are very close to the good-put value for the period of 10 seconds, while the grey values have significant variation from T_{10}. That means when PLRs are similar, trust values also tend to be similar, by using existed trust management schemes which choose PLR as the main parameter, though these schemes may process PLR with various formulas or algorithms, i.e., Bayesian approach. However, the new TMF described uses multiple parameters with Grey Theory to measure trust values. This is based on the assertion that any one node's behaviour, whether that interaction is successful or not, is affected by various factors, for example the node's signal strength, data rate, throughout, and delay. Therefore, the judgement on whether any node should be trusted, is not only determined by the probability of successful interactions, but also from various parameters in the physical and MAC layers.In fact, the packet loss rates of nodes *1, 2, 3* have little variance over the period, while the throughput and delay times of *node 1* are changing with time, compared with those of nodes *2 and 3*; this is shown in Figure 5. These changing parameters have a significant impact on the grey trust values.

4.4 Selfish behavior detection

The simulations were modified so that one node behaved selfishly. In operation, the node tends to be normal during the initial time, and then behaves selfishly, by only communicating with its nearby neighbours. Using Grey theory, the trust values are affected by the change in received signal strength, although the packet loss rate maintains the same value as with normal behaviours, this is shown in Figure 4. The main reason why the selfish node's trust value decreases is that its signal strength observed by the neighbour is increasing, leading to the drop in its signal strength grey value

Currently Grey Theory has been considered for use in developing trust models for wireless networks that have fixed topologies [8]. Some of these new trust models consider just three parameters; they also set fixed weight vectors for their input parameters in calculation of the Grey Relational Grade and the trust value; other research [10] uses Grey Theory in other aspects such as network selection, and not for distributed network trust management. A problem with using fixed weight vectors is that once attackers know which aspect is the most important factor in the system, the malicious nodes can obtain high trust values by only behaving well in that specified aspect, while in fact they do not cooperate with other normal nodes. In this paper, the new TMF considers a greater number of input parameters that cover all aspects of the lower level network protocols to calculate the trust values, hence making it more difficult for any malicious node to replicate all of them. Moreover, it uses several weight vector groups in order to obtain different trust values for a node; this can identify which aspect of a node's behaviour is abnormal, compared with other neighbour nodes. With this idea, the new TMF can also deduce selfish nodes' behaviour strategies.

Different weight vectors H may be used to calculate the grey value, and the new TMF uses multiple weight vectors from which it can calculate various trust values.

These different values can help to show differences between abnormal and normal behaviours; therefore in order detect the strategy that a selfish node employs, a range of vectors are used to identify the attempt to deceive the TMF. Figure 6 shows the results obtain when using the following vectors the : *H={0.2,0.2,0.2,0.2,0.2}* for (a), *H={0.6,0.1,0.1,0.1,0.1}* for (b), while *H={0.1,0.6,0.1,0.1,0.1}* for (c), and *H={0.1,0.1,0.1,0.6,0.1}* for (d), *H={0.1,0.1,0.1,0.1,0.6}* for (e), *H={0.1,0.1,0.6,0.1,0.1}* for (f). The weight configuration is such that for 5 input parameters, we use 6 vectors: one vector with equal weigh assigned to all input parameters, and 5 vectors each with one of the parameters having higher priority. Using this approach, we can not only detect general abnormal behavior, but also identify which of the input parameters are more responsible for it.

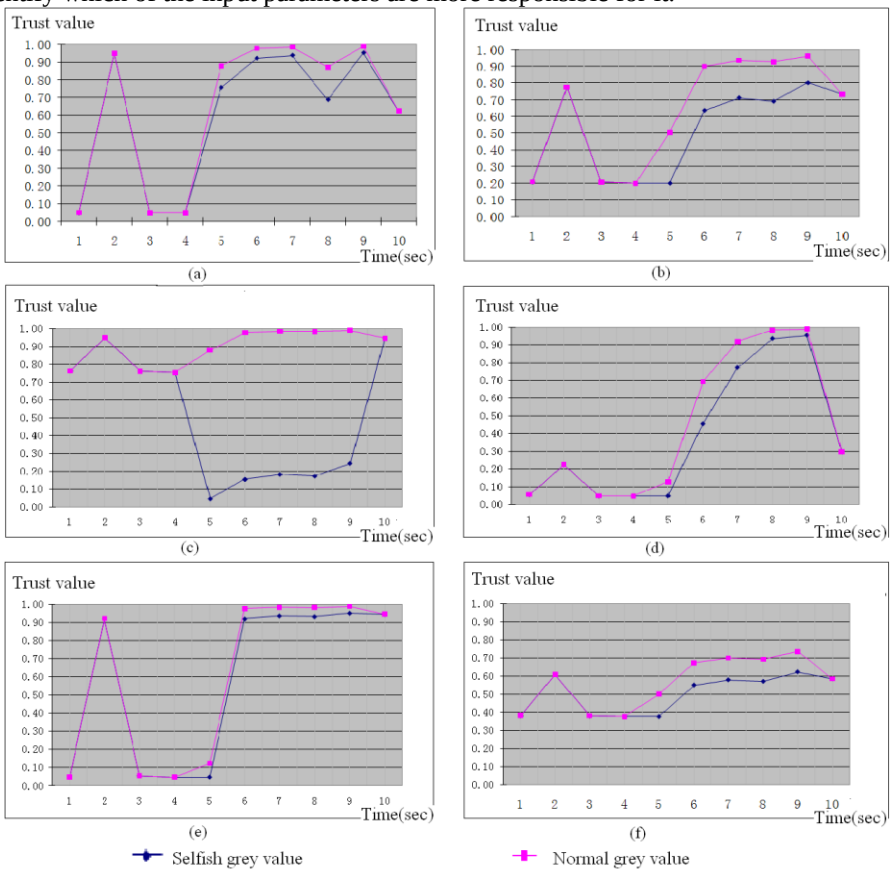


Figure 6 Different weight vectors (attack strategy detected in (c))

In Figure 6, the TMF sets different weight values for the signal strength and other parameters. The weight of signal strength is 0.2 Figure 6(a), 0.6 for Figure 6(c), while 0.1 for Figure 6(b), (d), (e) and (f). Generally, the system can find the difference in trust values between a normal node and a selfish one, when the five parameters have equal weight values, shown in Figure 6(a). Then, by using other weight vector groups, it can be clearly seen that there is a very large gap between normal and selfish trust values whenever the signal strength is set as the most important factor (weight value

0.6), in Figure 6(c). This reveals that the observed node is likely to be behaving selfishly on the aspect of signal strength, due to the abnormal value in Figure 6(c).
By setting the weight vectors, the trust management framework can detect more covert (intelligent) selfish behavior. For example, a node may maintain the packet loss rate at a normal level, but just cooperate with other nodes less frequently compared with normal nodes. By using the new framework, the results in Figure 7 (a) show that a selfish node with lower throughput results in a lower trust value, when setting *H={0.2,0.2,0.2,0.2,0.2}*. Moreover, if the framework uses H=*{0.1,0.1,0.1,0.1,0.6}*, it may be observed that the selfish behavior is largely linked with the parameter throughput, shown in Figure 7 (e). Similar results can be obtained for other selfish strategiies such as delaying packets.

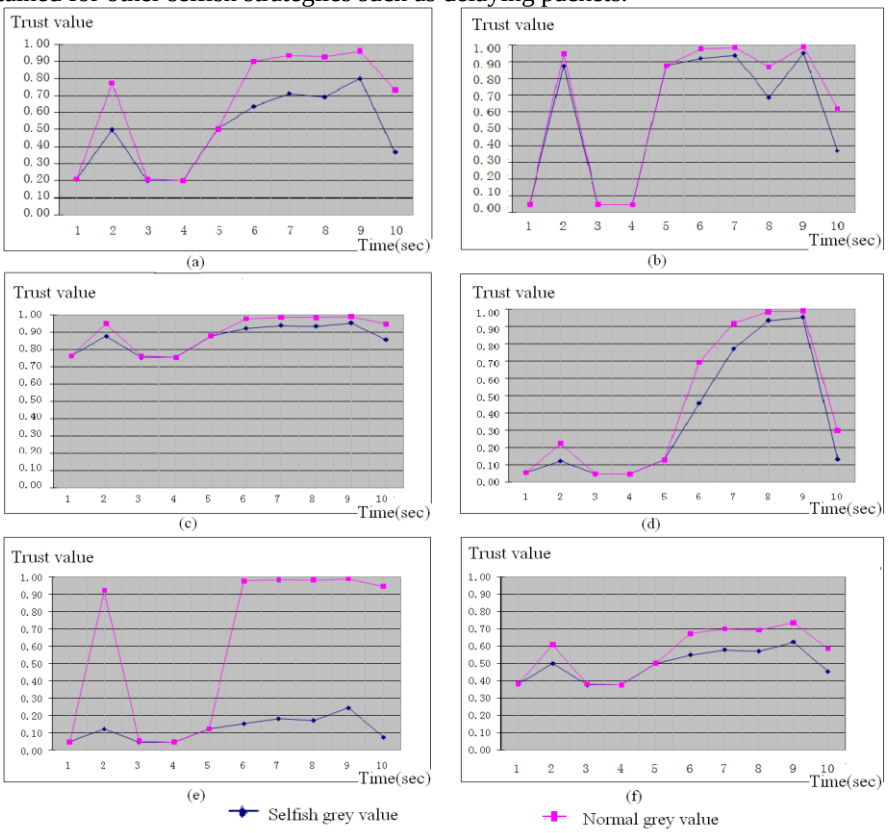


Figure 7 A selfish node's grey trust values (throughput behavior (e))

5 Conclusions

In this paper, a new trust management framework for ad-hoc wireless networks is presented. The new TMF employs multiple metrics to calculate a node's trust values rather than current approaches such as OTMF that consider only one parameter. The approach also uses Grey theory and Fuzzy sets to improve the trust value generation algorithms. Unlike other trust management frameworks, the TMF described in this

paper sets a weight vector for each of the input parameters. This provides a significant new benefit for the TMF as it can detect not only selfish or anomalous behaviour, but can also help identify the type of parameters used in the strategy of the attacker or selfish node.

Simulation results are presented that reveal the proposed framework can show clearly the difference in the trust values between a normal and selfish node on a specific parameter by setting an appropriate weight vector. In addition, the total trust value is calculated by using relation factors and weights of neighbour nodes, not just by simply taking an average value. Further research will test the proposed framework in more comprehensive environments with more network alternatives and selection criteria.

Acknowledgments. The authors would like to acknowledge the financial support from the China Scholarship Council (CSC) for this research. Also the authors would like to express their gratitude to Doctor F. Cai for offering useful information and constructive comments on the experiment studies this paper.

References

1. Jie Li, Ruidong Li, and Jien Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks", IEEE Communications Magazine, vol.46, no. 2, Apr. 2008, pp. 108-114.
2. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Proc. MobiCom 2002, Sept. 2002.
3. Huaizhi Li, and Mukesh Singhal, "Trust Management in Distributed Systems", IEEE Computer Society, vol. 40, Feb. 2007, pp. 45-53.
4. Yan Lindsay Sun, Wei Yu, Zhu Han, and K. J. Ray Liu, "Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks", IEEE Journal of Selected Areas in Communications (J-SAC), vol. 24, no. 2, Feb. 2006, pp. 305-317.
5. Trinh Anh Tuan, "A Game-Theoretic Analysis of Trust Management in P2P Systems", ICCE '06. First International Conference, Oct. 2006, pp. 130-134.
6. Zhiwei Qin, Zhiping Jia, and Xihui Chen, "Fuzzy Dynamic Programming based Trusted Routing Decision in Mobile Ad Hoc Networks, Embedded Computing", SEC '08 Fifth IEEE International Symposium on Embedded Computing, 2008, pp. 180-185.
7. Deng Julong, *Introduction to Grey Theory*, Wuhan: Huazhong University of Science & Technology Press, 2002.
8. Fu Cai, Tang Fugui, Cui Yongquan, Liu Ming, and Peng Bing, "Grey Theory Based Nodes Risk Assessment in P2P Networks", 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications, 2009, pp. 479-483.
9. Deng J., *A Course in Grey Systems*, Wuhan: Huazhong University of Science and Technology Press, 1990.
10. Qingyang Song, Abbas Jamalipour, "Network Selection in An Integrated Wireless LAN and UMTS Environment Using Mathematical Modeling and Computing Techniques", IEEE Wireless Communication, June 2005, pp. 42-48.
11. Yan Lindsay Sun, Zhu Han, and K. J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed networks", IEEE Communications Magazine, vol. 46, no. 2, Feb. 2008, pp. 112-119.
12. L. Hong, W. Chen, L. Gao, G. Zhang, and C. Fu, "Grey theory based reputation system for Secure Neighbor Discovery in Wireless Ad Hoc Networks", 2010 2nd International Conference on Future Computer and Communication (ICFCC), vol. 2, pp.749-754.
13. Sifeng Liu, and Yi Lin, *Grey Information: Theory and Practical Applications*, London: Springer-Verlag, 2006.