Fuzzy Logic based Trust Management in Mobile Ad hoc NET works

V. R. Ghorpade[1], Y. V. Joshi, R. R. Manthalkar[2]

[1]Asst. Prof., Kolhapur Institute of Technology, Kolhapur

[2] Professor, Shri Guru Govind Singh Institute of Engg. & Technology, Nanded

Abstract:

In order to advance the goal of anywhere anytime computing, the exposure to the risky transactions in mobile ad hoc networks has to be reduced as much as possible. This requires an existence of a trust management framework that enables nodes to form, maintain and exchange trust opinions. These opinions can then be used to customize the way interactions take place. A trust management framework for mobile ad hoc network (MANET) must be fully decentralized, highly customizable and selfish. In this paper, a fuzzy logic based trust management framework to establish, evaluate and propagate trust in MANET has been presented. In the proposed framework, trust is established by directly monitoring the evidences and obtaining fuzzy logic based recommendations from the neighboring nodes. A membership function is devised to take trust decision in a more accurate manner. This approach is optimistic in the sense that it allows more and more number of nodes to participate in network operations with different grades of trustworthiness. Mathematical analysis and simulations show that the proposed trust management framework can significantly improve the number of motivated nodes in the network which ultimately improves the network performance.

Keywords: Mobile ad hoc network, Trust management, Fuzzy logic.

1. Introduction

Rapid advances in wireless networking technologies have enabled mobile devices to be connected anywhere and anytime. An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to establish and maintain communications. On the move, applications on these nodes dynamically discover hosts and services with which interactions can be started. However, the fear of exposure to risky transactions with unknown entities may seriously hinder collaboration. In order to advance the goal of anywhere-anytime computing, the exposure to risky transactions has to be reduced as much as possible. This requires the existence of a trust management framework that enables nodes to form, maintain and exchange trust opinions. These opinions can then be used to customize the way interactions take place: for example which route to choose for sending data packets, detecting misbehaving nodes, key exchange and authentication etc.

A trust management framework for mobile ad hoc networks must be fully decentralized, as we cannot assume the existence of a trusted third party that can be contacted on demand to acquire reputation information about an entity. The framework must be highly customizable, in order to capture the varying and complex natural disposition of an individual to trust into computer models; this should be achieved without causing disruption to the device computation and communication resources. Finally a trust management framework for MANET must be selfish. In a resource constrained environment, selfishness is likely to prevail over cooperation, for example, to save battery power. A trust management framework cannot therefore completely rely on the assumption that entities have a social conscience that will make them exchange reputation information whenever asked.

Imprecision in data and information gathered from and about a mobile ad hoc network is either statistical or non-statistical. This later type of uncertainty is called fuzziness. Fuzzy models attempt to capture and quantify nonrandom imprecision. Hence, the focus of this paper is to develop a fuzzy logic based framework for establishing, evaluating and propagating trust in an ad hoc network without the use of cryptography. The establishment, evaluation and propagation of trust using fuzzy logic do not appear to have been seriously pursued in the literature.

This paper is organized as follows: In Section 2, a brief review of trust evaluation in ad hoc networks is presented. In Section 3, a fuzzy logic based trust management framework is proposed. In Section 4, mathematical analysis and simulation results have been discussed followed by concluding remarks in Section 5.

2. Review of trust evaluation in ad hoc networks

The research on trust evaluation has been extensively performed for a wide range of applications, including public key authentication, electronic commerce, peer-to-peer networks [1], [2], and ad hoc and sensor networks [3], [4], [5]. However there are still many challenges which need to be explored. Trust establishment and management between entities (nodes or agents) can be done through a central trusted authority or in a distributed fashion by nodes [6], or a combination of both. Related work in this area [5], [7], [8], [9], [10], employs both these techniques. For example, Zhou et al. [11] propose the idea of utilizing threshold cryptography to distribute trust in ad hoc networks, Davis [12] proposed the use of certificates based on hierarchical trust model to manage trust. Y. L. Sun et al. [13] proposed information theoretic framework of trust modeling and evaluation in which trust is measured by entropy. In [14] the trust evaluation process is formulated as a path problem on a weighted, directed graph. These approaches do not deal with the collection of evidence from the network, and the accompanying communication and signaling overhead; which need to be addressed. Kui Ren et al. [16] proposed a modified distributed trust establishment approach based on a secret dealer introduced only in system bootstrapping phase to simplify the process of trust initialization. C. Candolin et al. [17] proposed a method for distributing information regarding the trustworthiness of other nodes in the network. Trust is incomplete, that is, a node does not consider another node to be completely trusted or completely bad, but may describe the level of trust it has in another node.

A. A. Pirzada et al. [18] proposed a trust mechanism to discover routes which are used along with TORA protocol. In [19] an effort-return based trust model is used in a decentralized manner. It is influenced by swarm intelligence, where agents can solve complex problems through cooperation. In [20] effort-return based trust model is used to locate dependable routes in the presence of malicious nodes without making any superfluous assumptions. In [21] the concept of pure ad hoc network is used to introduce the notion of trust. By computing trust levels from the inherent knowledge present in the network, the trustworthiness of routes is computed. The proposed approach is novel and different from the existing ones in that no known schemes deal with establishment, evaluation and propagation of trust together. A fuzzy logic based approach is used for computing trust value. It has been proved that using fuzzy logic more accurate trust evaluation can be obtained, which further can be used for taking routing decisions and identifying misbehaving nodes.

3. Trust Management Framework

The proposed scheme is based on but different from existing work [15]. The trust management framework is made up of following three components [20]. Trust agent, recommendation agent and the combiner.

The trust agent derives trust levels from events that are directly experienced/monitored by a node. The recommendation agent shares trust information about nodes with other nodes in the network. The combiner computes the final trust in a node based upon the information it receives from the trust and recommendation agents. A schematic representation of the trust management framework is shown in Figure 1 below

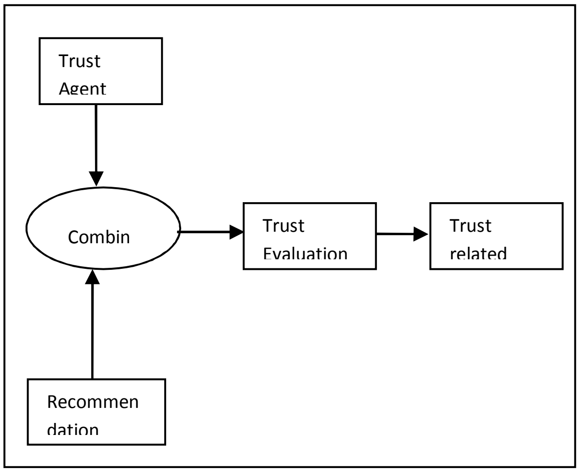

Fig. 1: Architecture of trust management framework

A. Trust Agent

The trust agent is an adaptation of the agent presented by Marsh [22] and has been specifically configured for use in ad hoc networks. Trust agents reside on every node and perform the task of trust derivation, quantification and computation. The agents monitor and log different context specific events in passive mode. Possible events that can be recorded in passive mode are the measure and accuracy of data and control packets that are either forwarded or received.

B. Recommendation Agent

The recommendation agent receives recommendations from nodes regarding their belief in other (REQUESTER) nodes. Similarly it sends its own recommendations to other requesting nodes (RECOMMENDER). The exchange of these recommendations between the REQUESTER and RECOMMENDER can be implemented periodically or on a request basis.

C. Combiner

The Combiner receives trust values from the Trust and Recommendation agents. To compute the total trust value of a target node, ET_{ab}, the combiner combines the fraction of direct trust T_{ab}, and fraction of recommendation, R_{ab} .System operation of proposed scheme is shown in Fig. 2.

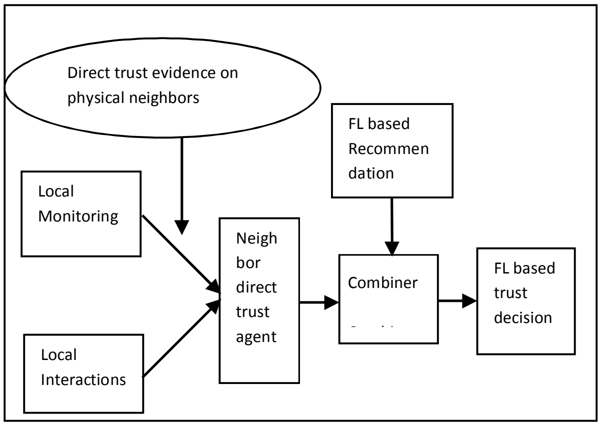

Fig. 2: System Operation

Following subsections describe the trust formalization through three different phases namely establishment, evaluation and propagation phase.

3.1. Establishment Phase

This is the phase when the network is newly deployed, or a new node joins the network. In a newly deployed network, nodes have no traffic statistics history about the network and their neighbors, and this is akin to the training or learning phase for the network. The scenario of a new node joining the network is similar, as the node does not have any trust information about its neighbors and vice-versa. During this phase, the new node(s) monitors its one-hop neighbors. The monitoring node switches over to promiscuous mode and listens for all packets transmitted by the monitored node. The new or unknown node is given a "bare" trust value.

During this phase nodes will not send sensitive data to their neighbors, unless timely delivery is absolutely essential (e.g. in disaster management scenarios it might be critical to exchange information immediately after network deployment). Time critical data is transmitted immediately utilizing flooding or any other techniques. All other information is buffered by the node till trust has been evaluated. Thus, proposed technique is a cautious combination of optimistic and pessimistic approaches. The nature and volume of critical data transmitted during this phase is strictly limited with the optimistic assumption that when the network is in startup phase, the probability of a malicious node assimilating enough information to compromise the network is very low. This is due to the relatively small amount of such data in the network versus the large volume of set up time control messages. It is also important to mention that this initiation phase lasts for a very short period of time and as soon as nodes have collected some information about their one-hop neighbors, they move to the evaluation phase.

3.2. Evaluation Phase

During this phase, the nodes evaluate their self-trust on their one-hop neighbors (i.e. T_{ab}) through monitoring system. Evaluation of the recommendation about the monitored node b ; by its neighbors R_{ab} is explained in the following subsections.

We define node a 's evaluated trust on another node b :

$$ET_{ab} = W_1 T_{ab} + W_2 R_{ab} \tag{1}$$

Where, ET_{ab} is evaluated trust on b by a

T_{ab} is node a 's self-evaluated trust on b ; a computes this by directly monitoring b . R_{ab} is an aggregation of recommendations made by other nodes on b evaluated by a . W_1 and W_2 are weights satisfying $W_1 + W_2 = 1$. Thus by varying W_1 and W_2 , a can vary the weight of self-evaluated versus recommendations in calculating its total trust on b .

Here, ($0 \le \{ET_{ab}, R_{ab}, T_{ab}\} \le 1$), and thus equation (1) is normalized.

3.2.1. Computing T_{ab}

Node a computes this value by directly monitoring b when b is in its radio range. Define T_{ab} as

$$T_{ab} = f(S, M) \tag{2}$$

Node' a s trust on b is a function f of traffic statistic functions S and M computed by monitoring b. Precise definition of f can be implementation dependent. Here, S is a function of monitored traffic statistics pertaining purely to traffic volume and M is a function of monitored traffic statistics pertaining to misbehavior. Here compilation of node monitoring statistics for one-hop neighbors is done. Thus, node a can monitor the following statistics for a one hop neighbor b.

▪ Data packets forwarded	s_1
▪ Control packets forwarded	s_2
▪ Data packets received	s_3
▪ Control packets received	s_4

- Packets dropped s_5
- Packets dropped due to unknown reason m_1
- Packets forwarding delay m_2
- Packets misrouted m_3

Now we can rewrite S and M as

$$S = g(s_1, s_2, s_3, s_4, s_5) \text{ and} \tag{3}$$

$$M = h(m_1, m_2, m_3) \tag{4}$$

Here, g and h are implementation dependent and they compute weighted summation of their constituent parameters.

3.2.2. Obtaining Recommendations

Here, take a set of nodes, N which are common and trusted neighbors of both a and b, into consideration. N is defined as :

$N = \{\forall$ node $n \in N \Rightarrow n$ is in the range of both a and b, and $\exists T_{an}$, such that $T_{an} \geq$ "*good*"$\}$ (5)

"*good*", is a threshold value for demarcating trustworthy and untrustworthy nodes. An algorithm as shown in Figure 3 is proposed for obtaining recommendations from node(s) $n \in N$ as defined in equation (5).

Algorithm: Recommendation Request (Node a needs recommendations about node b)

1. Node sends RECREQ to node(s).
2. If has recommendation for, then it will reply back with RECREP. While deciding the recommendation value, the concept of fuzzy logic is used here.
3. If does not have recommendation record for , then it will forward the RECREQ to its one-hop neighbors.
4. A max-hop and TTL field is maintained in RECREQ. The TTL field is decremented until it becomes zero and the max-hop field will be incremented by one, every time the RECREQ is forwarded to the next hop neighbors.

5. The max-hop limit is 2. After which RECREQ will not be forwarded. This is to reduce the communication and signaling overhead which comes into account while propagating the RECREQ and getting RECREP. The TTL can be few unit time.

Figure 3: Pseudo-code for Recommendation Request

3.2.3. Computing

Recommendation about trustworthiness is a subjective factor. Unlike the work discussed in Section 2, which use binary recommendation values; in this paper, recommendation grades have been used. Recommendation grades about a particular node are decided by other nodes considering its previous history of communication. Here, a parameter called experience statistics ( ) is used, which is a ratio of packets forwarded by packets received at a node, to decide the recommendation grade using fuzzy logic. To illustrate the concept and to find out a membership function hypothetical values of experience statistics are used as shown in Table 1.

Table 1: Experience statistics

% es	**Recommendation**	**Grade**
$es > 95$	Strong	1.0
$95 > es > 75$	Moderate	0.8
$75 > es > 55$	No comment	0.6

Proposed membership function $f(es)$ takes following values:

$$f(es) = \begin{cases} 1.0 & es \in [96{,}100) \\ o + p_1 \dfrac{(es - v) + 5}{5} & when \quad (v-5) < es < v \\ o & (v-20) < es < (v-5) \\ 0.0 & es \in (0{,}30] \end{cases}$$

(6)

Where, p_1 is a parameter that determines the rate at which, for each es, the function decreases with the increasing difference $|v - es|$. Let us assume that $p_1 = 0.2$, v is a variable and o is an $offset$. $\langle offset, v\rangle$ takes the values $\langle 0.8{,}95\rangle, \langle 0.6{,}75\rangle, \langle 0.4{,}55\rangle$ and

$\langle 0.2, 35 \rangle$. These values can be supplied by the user. Equation (6) is devised considering hypothetical data for a particular case. Hence, it is not a generalized equation.

By using equation (6), recommendation grade is obtained about a particular node in the range $[0,1]$. After obtaining the recommendations from different nodes the combiner can perform the aggregation of recommendations considering the security policy of the network. An aggregation strategy shown in Figure 4 is used in this paper.

```
if (security policy is high)
 then, $R_{ab} = \min\{r_{1b}, r_{2b}, ..., r_{nb}\}$ …………………………………..…………………(7)
  else if (security policy is low)

  then, $R_{ab} = \max\{r_{1b}, r_{2b}, ..., r_{nb}\}$

                                          …………………………………………(8)

else $R_{ab} = \frac{\sum_{i=1}^{n} r_{ib}}{n}$            ……………………………………………………..(9)    ----
------------------------------------------------------------------------------------------------------
```

Figure 4: Pseudo-code for aggregation strategy

where is the recommendation received about from th node, is the number of nodes giving recommendations and is the resulting recommendation grade which will be used in equation (1) for computing evaluated trust .

3.2.4. Trust Decision using Fuzzy Logic

In most of the trust evaluation methods discussed in Section 2, if the evaluated trust is greater than or equal to the threshold trust then that particular node is called as a trustworthy, else it will be treated as untrustworthy and excluded from all future network operations.

If the evaluated trust is very close to the threshold trust then such a node will also be excluded from the network operations. Since trust is a subjective concept, there can not be a bi-level demarcation as trustworthy and untrustworthy. We should trust such types of nodes; not fully, but at least by some percentile or grade. Depending upon the grade of trustworthiness the node can be included in the network operations and may be assigned different duties viz. send both the data and routing packets on one extreme and send only acknowledgement packets on the other extreme; through that node. A membership function is proposed here, which increases exponentially over the interval   of the evaluated trust computed by using equation (1). The function

$$tg(et) = \begin{cases} 1 & when\ et \geq tt \\ \dfrac{1}{1+(et-tt)^2} & when\ et \in (0, tt] \end{cases}$$

Where tg is trust valuation grade function, et is evaluated trust and tt is a threshold trust of a node. The outcome of the above function lies between $[0,1]$. We propose a policy for the inclusion of node(s) in the future network operations, as shown in Table 2.

Table 2: Trust evaluation grades

Trust Evaluation grade	Duties assigned to node(s)
1.0	Send both routing and data packets
0.9	Send only data packets
0.8	Send only routing packets
0.7	Send only acknowledge packets

3.3. Propagation Phase

Propagation or updating of the trust can be done by either proactive or reactive manner. In proactive case, as long as the monitored node remains in the radio range of the monitoring node, its trust is continuously evaluated and updated. This introduces the computational, communication and signaling overhead in the network. To make the updating process light weight, a reactive approach for trust updating can be used. In the reactive approach trust is updated only when demanded. The choice depends largely on the specific circumstances of the application and the network. For example, if local trust values change much more often than a trust decision needs to be made, then a proactive computation is not favored. The bandwidth used to keep trust values up to date will be wasted, since most of the computed information will be obsolete before it will be used. In this phase, three extremely different scenarios and their effect on trust propagation is taken into account.

i) Trusted one-hop neighbor move out of radio range due to node mobility. A node say,

i) b, which was previously in the radio range of a node a, now moves out of its radio range due to node mobility. The value of W_1 (the proportion of self-trust in overall trust) now decays exponentially as :

$$W_1 = Ce^{-\lambda t} \tag{11}$$

Parameter λ is the decay factor which is determined by the infrastructure and mobility constraints of the network, t is time and C is some constant. Node a now fixes T_{ab} to the value at time just before b moved away. But since W_1 exponentially decays, a's importance on T_{ab} in calculating ET_{ab} decreases with time. If the node b is outside a's radio range and if $ET_{ab} > T_{good}$ then, W_1 is forced to 0, and ET_{ab} is reduced to T_{good}. If the value of $ET_{ab} < T_{good}$ then it is left unchanged. This value of ET_{ab} is kept constant as the history information of node b; for the scenario that a and b eventually return to each other's radio range.

ii) Trusted one-hop neighbors that had previously moved out of radio range are now back in radio range. Node b, after moving out of a's radio range, eventually returns back in the range of a. Re-evaluation of ET_{ab} by a is now required for potentially restoring ET_{ab} to the highest trust value as b becomes directly monitored again. This re-evaluation does not begin from the bare trust value, but starts from the value of ET_{ab} previously fixed by a (after b had moved out of its radio range). Similar computations are done by b.

iii) The third scenario is when node b moves in the radio range of some other node n which is desirous to compute trust on b (i.e. ET_{nb}). In this situation node n can monitor node b for some time to compute T_{nb} and he can request for recommendations about b from its neighbors. Since a is neighbor of n and have maintained the trust record about its previous neighbor b; it can readily be made available to n. Thus trust about b can easily be propagated in the network.

4. Mathematical and Simulation Analysis

4.1. Mathematical Analysis

For the mathematical analysis, it is assumed that there are 102 nodes in the network. From these nodes one of the nodes (monitoring node a) wants to obtain recommendations about another node (monitored node b); from rest of the nodes in the network. which itself means that about 100 nodes are present for giving recommendations. From these 100 nodes 50% of the nodes have a very good (100% es - experience statistic) prior experience with the monitored node. 10% of the nodes have slightly less (95% es) experience statistics value. Now, it has been observed that fuzzy based approach plays a crucial role in deciding the recommendation grade about a particular node. It is assumed that if the experience statistics value related with a node is greater than 80% then that node is a *Trustworthy* (T) node otherwise it is Untrustworthy (UT) in a bi-level (BL) method of giving recommendations. Table 3 shows the improvement in the number of nodes giving recommendation with different grades which can then be aggregated to obtain resulting recommendation about a node in question.

Table 3: Obtaining recommendations

Nodes	*es*	BL Rec.	FL Rec.	*es*	BL Rec.	FL Rec.
50	100	T	1.0	100	T	1.0
10	95	T	1.0	85	T	0.8
10	85	T	0.8	75	UT	0.6
10	75	UT	0.6	70	UT	0.6
10	65	UT	0.6	60	UT	0.6
10	55	UT	0.6	55	UT	0.6

From the above table it is clear that, if bi-level decision technique is used for obtaining recommendations then the numbers of nodes participating in network operations are less as compared with the fuzzy logic based technique. In case of fuzzy logic based technique, nodes having different grades of trustworthiness are used for different applications. If the value is greater than or equal to the threshold which is set for deciding the recommendation value, then the neighboring node(s) will strongly recommend the monitored node else it will not recommend the node (a bi-level logic). Column 4 and 7 in Table 3 are computed using equation (6). By observing these two columns it can be said that, depending upon the value of the recommendation grade about the monitored node changes. Such recommendation grades have been obtained and the resulting recommendation value is computed by using the aggregation strategy shown in Figure 4. Further, recommendation value is used in equation (1) to compute the evaluated trust on the monitored node.

Assume that the threshold trust value for monitored node is 0.8. In a bi-level approach, the evaluated trust which is computed in equation (1) is compared with the threshold trust of the monitored node and the trustworthiness of the node is decided. Depending upon this decision the node will be included or excluded from the network operation.

In this proposed approach, equation (10) is used to compute the trust grade. Depending upon the outcome of equation (10) the monitored node will be assigned appropriate duties in the network as illustrated in Table 2. Therefore, from Table 3, it can be concluded that, if a bi-level (BL) approach is used for trust evaluation around 70 to 60 percent nodes will take part in the network operations. But, when the fuzzy logic (FL) based technique is used then almost 100 percent nodes take part in network operations, but of course, with appropriate; however small it is, duties.

Table 4: Trustworthiness

Security Policy	Trustworthiness about node b			
	BL	FL	BL	FL
High	UT	UT	UT	UT
Moderate	UT	T	UT	T
Low	T	T	T	T

Table 4 shows that, if a bi-level technique is used for trust decision then node can participate in network operations only when the security policy of the network is low. On the other hand if a fuzzy logic based approach is used then node can participate in network operations whenever the security policy is low or moderate. This shows that, the proposed approach is optimistic and motivates the nodes to participate in network operations and gain rewards which, they can use for improving their reputation for future.

4.2. Simulation Details

The purpose of simulation is to show how the number of nodes participating in the network operation increases when we use the approach proposed in this paper. For simulation, Network Simulator (ns-2) [23] is used. A network having 100 mobile nodes is considered, in which the nodes are moving with a speed of 2 m/s on a flat area admeasuring 800X800 m2. The number of traffic source and sink pairs are ten. The UDP/CBR and TCP/FTP type traffic has been simulated. The packet size is 512 bytes and the routing protocol used is AODV. The simulation is run for 100 unit times.

4.3. Observations and Discussions

Different sets of observations are taken and it is observed that the fuzzy logic based approach overweighs the bi-level approach in evaluating the trustworthiness of the nodes under consideration.

5. Conclusion

In this paper, the objective of establishing a fuzzy based framework for evaluating and propagating trust in mobile ad hoc networks is fulfilled. It is observed that, if a particular node is very close to the threshold limit of deciding recommendation, then in this optimistic approach, that node will be pulled up/motivated to participate in the network operations. If it gets involved in the network operations it will get a chance to build its reputation. Otherwise, if such a node is kept away, it will not get a chance to build its reputation and hence gets de-motivated. During the network running phase our objective is to include more and more nodes in network operations giving due importance to the security policy of the network. If the policy is pessimistic, then the number of de-motivated nodes increase which will ultimately degrade the performance of the entire network.

References

[1] P. R. Zimmermann, The Official PGP User's Guide, Cambridge, MA:MIT Press, 1995.

[2] B. Yu, M. P. Singh, and K. Sycara, “Developing Trust in large-scale peer-to-peer systems,” in Proc. 1st IEEE Symp. Multi-Agent Security and Survivability, pp. 1-10, 2004.

[3] K-W Kim, J-C Jeon and K-Y Yoo, “Efficient and Secured Password Authentication Schemes for Low-Power Devices ,” Mobile and Sensor Networks, LNCS 3794, pp. 73-82, 2005.

[4] P. Michiardi and R. Molva, “CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” Technical Report, Institute Eurecom, France.

[5] G. Theodorakopoulos and J. S. Baras, “Trust Evaluation in ad hoc Networks,” Proc. of ACM Workshop on Wireless Security, pp. 1-10, 2004.

[6] A. Rahman and Hailes, “A Distributed Trust Model ,” Proc. of the 1997 New Security Paradigms Workshop- ACM Press, pp. 48-60, 1997.

[7] D. Balfanz, D. K. Smetters, P. Stewart and H. Chi Wong , “Talking to Strangers: Authentication in Ad Hoc Wireless Networks,” Symposium on Network and Distributed Systems Security, 2002.

[8] J. Kong, H. Luo, K. Xu et al., “Adaptive Security for Multi-Layer Ad Hoc Networks,” Special Issue of Wireless Communications and Mobile Computing , 2002.

[9] T. Huges, J. Denny, P. Muckelbauer, J. Etzl, “Dynamic Trust Applied to Ad Hoc Network,” Resources Autonomous Agents and Multi-Agents Systems Conference, Melbourne, Australia, 2003.

[10] J. Kong, P. Zerfos, H. Luo et al., “Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks,” Proc. of International conference on Network Protocols (ICNP), pp. 251-260, 2001.

[11] L. Zhou and Z. J. Hass, “Securing Ad-Hoc Networks,” IEEE Network, Vol. 13, No. 6, pp. 24-30, 1999.

[12] C. Davis, “A localized Trust Management Scheme for ad hoc networks,” Proc. of 3rd International Conference on Networking, 2004.

[13] Yan L. Sun, Wei Yu, Zhu Han et al., "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 305-317, 2006.

[14] T. George and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 318-328, 2006.

[15] M. Virendra, M. Jadliwala et al., "Quantifying Trust in Mobile Ad Hoc Networks," IEEE International Conference on Integration of Knowledge Intensive Multi-Agent Systems, pp. 65-70, 2005.

[16] Kui Ren, T. Li, Z. Wan et al., "Highly Reliable Trust Establishment Scheme in Ad Hoc Networks," Preprint submitted to Elsevier Preprint, 2004.

[17] C. Candolin and H. H. Kari, "Distributing Incomplete Trust in Wireless Ad Hoc Networks," Proc. of IEEE Southeast Conference, pp. 68-72, 2003.

[18] A. A. Pirzada, C. McDonald, "Trusted Route Discovery with TORA Protocol," Proc. of the Second Annual IEEE Conference on Communication Networks and Services Research.

[19] A. A. Pirzada, A. Dutta, C. Mcdonald, "Trusted Routing in Ad Hoc Networks using Pheromone Trails," IEEE, pp. 1938-1943.

[20] A. A. Pirzada, A. Dutta, "Propagating Trust in Ad Hoc Networks for Reliable Rou ting," IEEE International Workshop on Wireless Ad Hoc Networks, pp. 58-62, 2004.

[21] A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad Hoc Networks," Proc. of 27th Australasian Computer Science Conference, 26(1), pp. 47-54, 2004.

[22] S. P. Marsh, Formalizing Trust as a Computational Concept, Ph.D. Thesis, Dept. of Mathematics and Computer Science, University of Stirling, 1994.

[23] ns-2 (The Network Simulator). [Online] http://www.isi.edu/nsnam/ns/