# TRUST ORIENTED SECURITY FRAMEWORK FOR AD HOC NETWORK

Amandeep Verma[1] and Manpreet Singh Gujral[2]

[1]Punjabi University Regional Centre for IT & Mgmt., Mohali, INDIA
[2]University College of Engineering, Punjabi University, Patiala, INDIA

## ABSTRACT

*An ad hoc network is a group of wireless mobile hosts that are connected momentarily through wireless connections in the dearth of any centralized control or some supporting services. The mobile ad hoc network is at risk by its environment because of the vulnerabilities at channel and node level. The conventional security mechanisms deals with only protecting resources from unauthorized access, but are not capable to safeguard the network from who offer resources. Adding trust to the on hand security infrastructures would improvise the security of these environments. A trust oriented security framework for adhoc network using ontological engineering approach is proposed by modeling ad hoc network, the OLSR (Optimized Link State Routing) protocol and trust model as OWL (Ontology Web language) ontologies, which are integrated using Jena. In this model, a trustor can calculate its trust about trustee and use the calculated trust values to make decisions depending on the context of the application or interaction about granting or rejecting it. A number of experiments with a potential implementation of suggested framework are performed to validate the characteristics of a trust oriented model suggested by the literature by this framework*

## KEYWORDS

*Ad hoc Network, Framework, Ontology, Trust*

## 1. INTRODUCTION

An ad hoc network is a group of wireless mobile hosts that are connected momentarily through wireless connections in the dearth of any centralized control or some supporting services. It is worth to mention that ad-hoc networks are not an alternative or substitution of the networks with infrastructures. Their extent is in the locale where cost, environment, or application constraints require self-organized and infrastructure-less solutions [18]. The mobile ad hoc network is at risk by its environment and the various vulnerabilities [3] that exist in the mobile ad hoc networks are

- *Channel vulnerability*: broadcast wireless channels can cause message eavesdropping and injection.
- *Node vulnerability*: nodes lack physically protected places, thus susceptible to attacks.
- *Absence of infrastructure*: certification/ authentication authorities are missing.
- *Dynamically changing network topology* puts security of routing protocols under threat.
- *Power and computational limitations* prevent the use of complex encryption algorithms.

With constraint on access to only certified users, resources are protected from malicious users in the customary security mechanisms. Though there are numerous circumstances where is need to shield from those who offer resources, the quandary is inverted. For example, information providers may act maliciously by providing deceptive or counterfeit information. Moreover the conventional security mechanisms are not able to guard the network from such type of attacks

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 19–26, 2012.

DOI : 10.5121/csit.2012.2203

[17]. Adding trust to the existing security infrastructures would enhance the security of these environments [11]. Trust concept is more applicable to ad-hoc networks because:

- The quite dynamic nature of the ad hoc network makes it difficult to grant the behavior definitely.
- The proposition "something is good" will be changed to "I think something is good". The opinion is changed to subjective view from objective view [4].

Within the sphere of network security, the elucidation of the theory of trust is as a relation amid entities that partake in various protocols. Trust relations are substantiated by the preceding interactions of entities within a protocol [12]. It was revealed from the review of literature presented in section 2 that nearly all of the studies include the trust in order to improve the performance of some existing protocol or the newer or modified methodology for trust evaluation.The studies vary in the process of trust evaluation, trust updation and trust propagation. Some of the studies are at variance in the terms of initial trust evaluation. The assimilation of these trust evaluation processes to an existing ad hoc network is different in terms of the network layer to which these are functional and the level of abstraction it provided to the whole network.Accordingly it is concluded that a framework is missing that will provide the researchers with a template where they endow with their own method for trust evaluation, updation and even propagation with same environment for the rest of the network. This proposal can be used to compare the various trust evaluation mechanisms. The purpose of our study is to develop a framework as stated above that helps in building the trust oriented secure ad-hoc network environment.

In order to efficiently design and engineer trust networks, ontologies create a methodology and mechanism to describe trust relations and their sub-components [1].The ontological engineering approach was used to build the framework.

## The Perspectives

Trust-oriented security framework, in order to secure the network from malicious behaviors of the nodes, can be used in making decisions for the following perspectives such as

### *Application Execution*

While the ad hoc network is in operation, numbers of applications like email, instant messaging, ftp and many others have to be started by the nodes in the network. As all of the participating nodes are ad hoc in nature so it is advisable to ensure the validity of the target node before staring any type of application execution as an interaction with the target node.

### *Routing Environment*

While the ad hoc network is in operation, there is a lot of packet flows over the network. The packet follows the path as per the routing protocol from node to node. In this context before forwarding the packet the source first gets the trust value on the receiver and is allowed to forward only if the trust value is above the threshold specified as per the policy. As the trust value is the result of past interactions so any misbehaving node can be excluded by this validation on the basis of trust.

### *Authentication*

To accept or reject a public key certificate depends on the trust value of introducing node. Therefore the nodes involved in decision making is the value of trust that node s has on the originator.

*Pick the Best*

Sometimes there is possibility the nodes have number of options i.e. number of nodes in the network, for an interaction or getting a service from it. In order to select among them, one of the criteria is to go ahead with the node for which the initiator has the highest trust value. So it leads to choosing the best among the available choices.

The paper is organized as follows. The section 2 is about the review of literature about the trust in ad hoc networks. The section 3 gives the outline of the framework and section 4 is about the discussions.

## 2. REVIEW OF LITERATURE

An adhoc routing protocol [5] TAODV (Trusted AODV) extends the widely used AODV (ad hoc on-demand distance vector) routing protocol and employs the idea of a trust model to protect routing behaviors in the network layer of MANETs. In the TAODV, trust among nodes is represented by opinion, which is an item derived from subjective logic. Because of the dynamic nature of adhoc networks, trust evidence may be uncertain and incomplete. A Trust-Domain based security architecture [16] for mobile ad-hoc networks is twofold: to use trust as a basis to establish keys between nodes, and to utilize trust as a metric for establishing secure distributed control in infrastructure-less MANETs. The metrics for nodes to establish and manage trust, and use this mutual trust to make decisions on establishing group and pair-wise keys in the network are defined. An information theoretic framework [19] to quantitatively measure trust and model trust propagation in ad hoc networks is proposed. In the proposed information theoretic framework, trust is a measure of uncertainty with its value represented by entropy. Axioms are developed that address the basic rules for trust propagation. Based on these Axioms, two trust models are presented: entropy-based model and probability-based model, which satisfy all the Axioms. Simulations show that the proposed framework can significantly improve network throughput as well as effectively detect malicious behaviors in ad hoc networks.

A cluster-based trust model [7] against attacks in adhoc networks was proposed. The reputation from a neighboring node is applied to the calculation of the trust value. If the trust value of a trustier is used as a weight, more sophisticated calculation of the trust value is available. When one create a cluster, all nodes in the cluster can fully trust the selected head, if entire nodes in the cluster participate in the head competition. And then, the head node issues the certificate that shows the trust level of each member node. If a node moves from one cluster to another, the trust level of the node is determined by the certificate issued by the previous cluster-head. A paper [15] analyze human based trust model for adhoc networks. They aim at building a trust relationship among nodes, confining the interactions to direct neighbors to better scale on mobile networks. They provide a mechanism for nodes to evaluate the trust level of their neighbors. They also analyze the advantages of considering the relationship maturity, i.e. for how long nodes know each other, to evaluate the trust level.

## 3. THE FRAMEWORK

### 3.1 The Design

A framework is to outline probable lines of acts or to depict a favored approach to a proposal or notion. A framework can work that is approximating to a plot giving reasoning to pragmatic inquisition. For software development point of view, a framework, that is used by software developers to implement the standard structure for an application. An excellent framework should be conceptual and absolute, obvious and definite, summarized and comprehensible, straightforward to sustain and cost efficient. Above all, it should be valuable. An abstract representation of the proposed framework is shown in Fig 1.

The Ad hoc Network Set Up should have the description classes essentially- network parameters, application and the node parameters. An exhaustive study of the literature and simulation tools for ad hoc networks acknowledged the subsequent network parameters—Geographical Area, Number of Nodes, Placement of nodes, Mobility model, Terrain and some other optional parameters. The application class expresses the catalog of possible applications that can be accomplished e.g. Email, ftp, chatting, video conferencing and so on. The node parameters are used to depict the parameters of node in provisions of battery, memory, mobility speed, clock speed.

The trusted protocol is an enhanced adaptation of an existing protocol. The protocol may be a routing protocol, or an authentication protocol or an access control protocol. Thus this flexibility in the proposed framework results it as a generalized framework. The protocol is customized so that it should take trust value in concern while making decisions. We have presented a relative study of performance of ad hoc routing protocols in our prior work [13]. On the source of the results of that study we have selected the OLSR routing protocol for demonstrative purposes. Subsequent to the selection of protocol, the next step is to make it trusted protocol. The formal specifications of the trusted OLSR protocol in formal language Z is given in the paper [14]. The trusted protocol with the ad hoc network setup granted a trusted ad hoc network i.e. an ad hoc network that too considers trust value while making decisions.

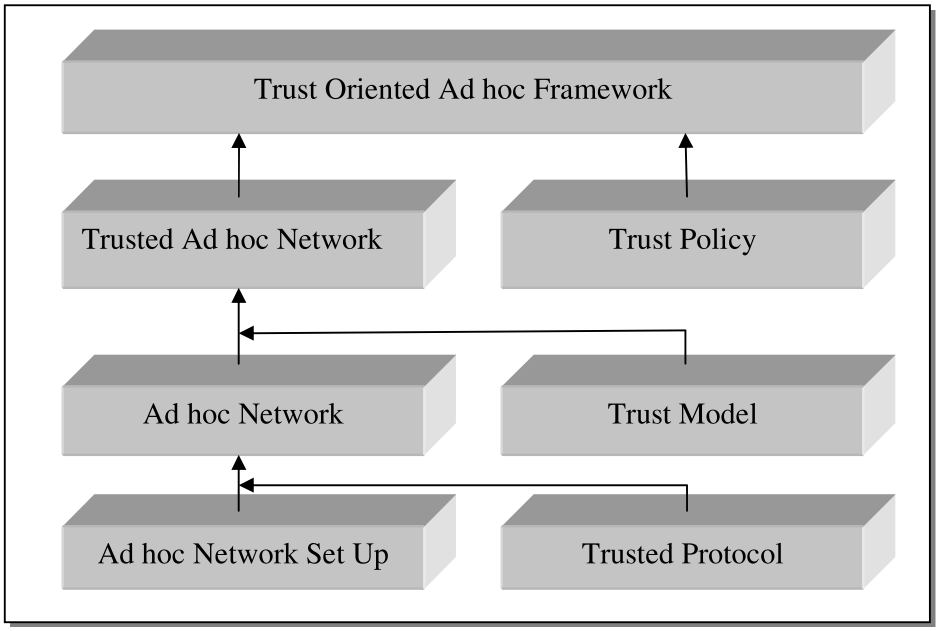


Figure 1: Abstract Representation of Trust oriented Ad hoc Network Framework

The trust model is intended to work as a trust service. This service is accountable for the trust evaluation, trust updation and trust propagation. The trust model encompassed the following components – Trust Configuration, Trust Assessment and Trust Appliance. The trust configuration in essence engrosses-- characterizations of trust relationships, a range of trust categories, probable trust values. The trust assessment module is accountable for the trust evaluation. The trust appliance entailed the supply of trust values to the calling module. A trust value is a compute or quantification assigned by a source unit to its confidence in the trustworthiness of target unit. The trust value often signifies the prospect of a successful interaction, through which some desired outcome will be attained [2]. This trust service is called for in the situation where the recommendation from the rest of the nodes in the network is required by a node in the network. The trusts on recommendations are largely classified into two sorts- direct trust and indirect trust. The direct trust a node has on the basis of its own experience and indirect trust on the basis of other's node experience with the node in question. The alternatives available in the projected framework for trust evaluation purposes are

Risk or Context of the Operation/Application i.e. No Risk, Low Risk, Medium Risk, High Risk and Highest Risk application

Global Trust or Local Trust.

Different or Same weights to recommendations

The risk or context is defined with the operation or application on run. The purpose of associating it is required as the trust requirement to allow or disallow any operation depends on the requirement of the context associated with the application e.g. Low risk applications are allowed even with the low value of trust and on the other hand high trust value is required for high risk applications. The preference of Global Trust and Local Trust is made available as many researchers either prefer global or local trust depending on their means of trust evaluation and the same notion is behind in presenting the weight option to recommendations.

The trust policy adopted to allow or discard an interaction on the basis of trust and the context of the application. As the policy varies and it is largely dependent on the area of application of the ad hoc network, so this is the constraint that it should be abstract from the rest of the environment.

## 3.2 The Approach

Nowadays, ontologies are used into an extensive range of applications. Besides the Semantic Web, they are even functional to knowledge management, content and document management, information and model integration, etc [8]. The researchers who need to share information are provided with common vocabulary by the ontology [6]. The machine-interpretable descriptions of fundamental concepts in the domain and relations along with them are presented by it. The ontology structure the glossary by defining the central vocabulary and relations to model a domain. These glossaries are used in creating knowledge bases, developing services that function on knowledge bases and building system that are combination of these knowledge bases and services [10]. The process of developing ontology is analogous of the description of set of data and their composition for further programs to exercise. Each ontology O contains a set of concepts (classes) C and a set of properties P. A class is a collection of individuals and a property is a collection of relationships between individuals (and data). Individuals are the specific concepts. The relation between an individual to another individual is represented by property called an object property. The datatype property is specified to depict the mapping of an individual to a data literal. Every property has domain and range as the other mathematical functions. While both domain and range of object properties are ontology classes, the range of datatype properties are data literals such as integer, time, etc.

### 3.2.1 The Implementation

The OWL (Ontology Web language), which is recommended by W3C (World Wide Web Consortium), is used to model ad hoc network, the OLSR (Optimized Link State Routing) protocol and trust model as OWL (Ontology Web language) ontologies using Protégé ontology development tool. To present the framework these ontologies are integrated using Jena. The snapshots of the interface and of ontology description are shown in Figure 2 and Figure 3.

.

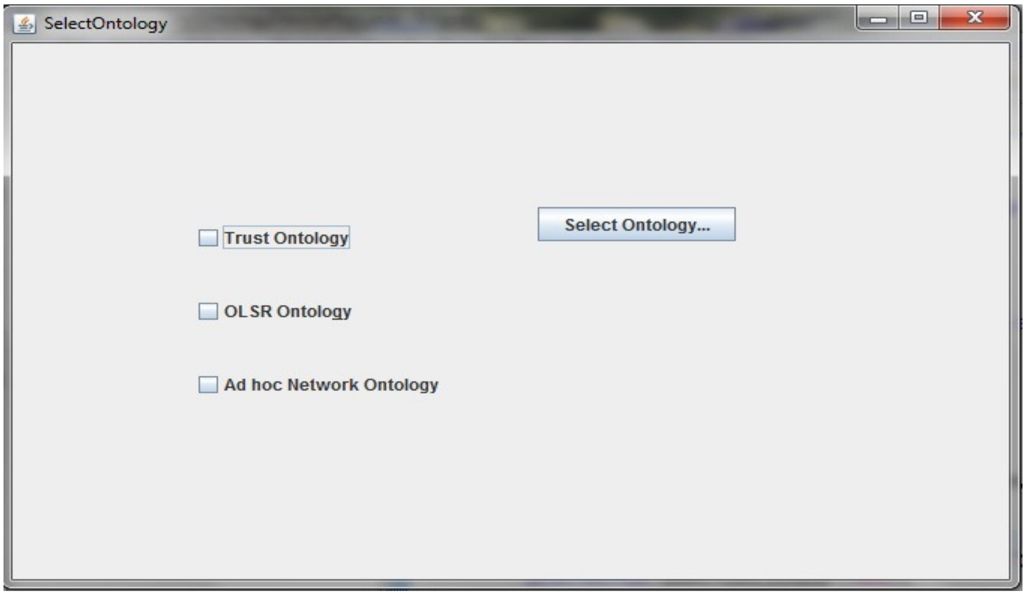
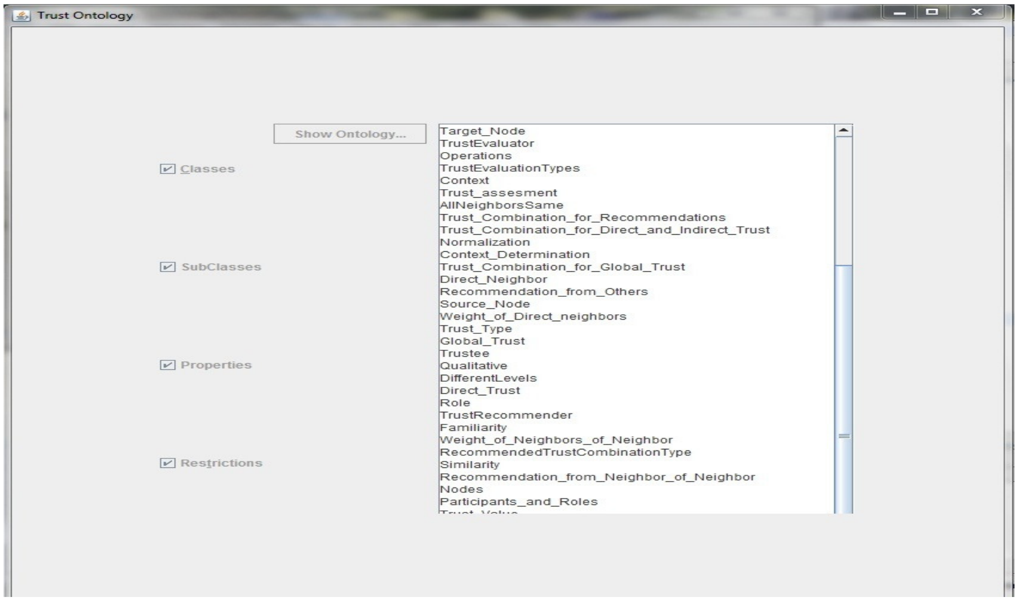


Figure 2: A Snapshot of the Interface



☑ Classes

☑ SubClasses

☑ Properties

☑ Restrictions

```
Target_Node
TrustEvaluator
Operations
TrustEvaluationTypes
Context
Trust_assesment
AllNeighborsSame
Trust_Combination_for_Recommendations
Trust_Combination_for_Direct_and_Indirect_Trust
Normalization
Context_Determination
Trust_Combination_for_Global_Trust
Direct_Neighbor
Recommendation_from_Others
Source_Node
Weight_of_Direct_neighbors
Trust_Type
Global_Trust
Trustee
Qualitative
DifferentLevels
Direct_Trust
Role
TrustRecommender
Familiarity
Weight_of_Neighbors_of_Neighbor
RecommendedTrustCombinationType
Similarity
Recommendation_from_Neighbor_of_Neighbor
Nodes
Participants_and_Roles
```

Figure 3: A Snapshot of the Ontology Description

## 4. DISCUSSIONS

The main features of trust in MANETs summarized in [9] on the basis of the review of various studies. These features and the corresponding validation of these features in our proposed model are shown in the Table 1.

Table 1: Features of Proposed Framework

| S. No | Features of Trust in MANET [9] | Features of Proposed Framework |
|---|---|---|
| 1. | A decision method to determine trust against an entity should be fully distributed | The final trust value depends on the recommendations of all the nodes of the network and hence fully distributed approach |
| 2. | Trust should be determined in a highly customizable manner without excessive computation and communication load, while also capturing the complexities of the trust relationship | There is no need for a node to request and verify certificates before interaction and therefore greatly reduces the computational overheads. By introducing context “NoRisk”, trust evaluation of such interactions avoided. Even more for “LowRisk” interaction the “local trust” rather than “Global Trust” evaluation is sufficient, again reducing the computation load of trust evaluation |
| 3. | A trust decision framework for MANETs should not assume that all nodes are cooperative. | Even if some of the nodes are non-cooperative, the trust value on the bases of other nodes gets calculated |
| 4. | Trust is dynamic, not static. | The trust increases on successful interaction and decreases on unsuccessful interaction and hence dynamic |
| 5. | Trust is subjective | Trust is subjective as it depends on recommendations and even on the context |
| 6. | Trust is not necessarily transitive. | The trust depends on direct experiences as well indirect experiences individually. The weightage of the recommendation for indirect experience depends on the location of the node, so no transitivity in trust |
| 7. | Trust is asymmetric and not necessarily reciprocal. | The neighborhood of a every node is different and hence the weighting factor of the recommender node is also different and hence the trust is asymmetric |
| 8. | Trust is context-dependent | Trust decision depends on the context of the interaction, that is defined in terms of the degree of risk |

## REFERENCES

[1] Dokoohaki Nima and Matskin Mihhail, “Effective Design of Trust Ontologies for Improvement in the Structure of Socio-Semantic Trust Networks ,” International Journal on Advancements in Intelligent Systems, Vol. 1, Issue1, pp 23-42, 2008.

[2] Glenn Mahoney, Wendy Myrvold and Gholamali C. Shoja, “Generic Reliability Trust Model”, Proceedings of the 3rd Annual Conference on Privacy, Security and Trust, pp. 113-120, 2005

[3] Li Wenjia and Joshi Anupam ,” Security Issues in Mobile Ad hoc networks (A Survey)”, The 17th White House Papers Graduate Research In Informatics at Sussex, pp.1-23, 2004.

[4] Li Xiaoqi, “Evaluating Trust in Ad hoc Networks,”
http://www.cse.cuhk.edu.hk/~lyu/seminar/06spring/gigi.pdf

[5] Li Xiaoqi, Lyu, M.R. and Liu Jiangchuan, “ A Trust Model Based Routing Protocol for Secure Ad Hoc Networks”, Proceedings of IEEE Aerospace Conference, vol. 2, pp. 1286-1295, 2004

[6] Mizoguchi R. “Tutorial on ontological engineering,” http://www.ei.sanken.osaka-u.ac.jp/pub/miz/Part1-pdf2.pdf

[7] Park Seong-Soo, Lee Jong-Hyouk and Chung Tai-Myoung, "Cluster-Based Trust Model against Attacks in Ad-Hoc Networks", Third International Conference on Convergence and Hybrid Information Technology, vol. 1, pp.526-532, 2008

[8] Plessers Peter and Troyer Olga De, “Resolving Inconsistencies in Evolving Ontologies,” Y. Sure and J. Domingue (Eds.), ESWC 2006, LNCS 4011, pp. 200-214, 2006

[9] Ramana K.Seshadri, Chari A.A., Kasiviswanth N., “A Survey On Trust Management For Mobile Ad Hoc Networks,” International Journal of Network Security & Its Applications, Volume 2, Number 2, pp. 75-85, April2010

[10] Robert Neches, Richard Fikes, Tim Finin, Thomas Gruber, Patil Ramesh, Senatoe Ted and William R. Swartout, “Enabling Technology for Knowledge Sharing,” AI Magazine, pp. 37-56, Fall 1991

[11] Taherian M., Jalili R. and Amini, M., “PTO: A Trust Ontology for Pervasive Environments,” Proceedings of International Conference on Advanced Information Networking and Applications, pp. 301-306, 2008

[12] Theodorakopoulos G. and Baras J.S., “On trust models and trust evaluation metrics for ad hoc networks,” IEEE Journal on Selected Areas of Communication, Vol. 24, Issue 2, pp. 318 – 328, 2006

[13] Verma Amandeep and Gujral Manpreet Singh, “Performance Analysis of Routing Protocols for Ad hoc Networks,” International Journal of Computer Science and Emerging Technologies, Vol. 2, No. 4, pp. 484-487, August 2011, Published by ExcelingTech Publisher, UK

[14] Verma Amandeep and Gujral Manpreet Singh, “Formal Specifications of Trusted OLSR Protocol of Ad hoc Network in Z,” International Journal of Computer Applications 37(2):25-36, January 2012. Published by Foundation of Computer Science, New York, USA

[15] Velloso P.B., Laufer R.P., Duarte O., and Pujolle G, “Analyzing a Human-based Trust Model for Mobile Ad Hoc Networks”, IEEE Symposium on Computers and Communications, pp. 240-245, 2008

[16] Virendra Mohit, Jadliwala Murtuza, Chandrasekaran Madhusudhanan and Upadhyaya Shambhu, “Quantifying Trust in Mobile Ad-Hoc Networks”, Proceedings of IEEE conference on Integration of Knowledge Intensive Multi Agent Systems, pp. 65-70, 2005

[17] Wang Yufeng, Hori Yoshiaki and Sakurai, Kouichi, “Economic-Inspired Truthful Reputation Feedback Mechanism in P2P Networks,” IEEE International Workshop on Future Trends of Distributed Computing Systems, pp. 80-88, 2007

[18] Weimerskirch Andr´e and Thonet Gilles, “A Distributed Light-Weight Authentication Model for Ad-hoc Networks,” Proceedings of International Conference on Information Security and Cryptology, pp. 341-354, 6-7 December 2001

[19] Yan Sun, Wei Yu, Zhu Han and Liu K.J.R., “Trust modeling and evaluation in ad hoc networks”, Proceedings of IEEE conference on Global Telecommunications, vol. 3, pp. 6, 2005