I J C T A, 8(5), 2015, pp. 1735-1742

Trust-based multi-path Security Scheme for Ad-hoc networks

C.K. Shyamala*, Niveda Ashok & Bhavya Narayanan*****

Abstract: Open and autonomous environments are highly heterogeneous and are characterized heavily by entities that leave or join the community as they choose. Security is termed as the degree of resistance to, or protection from, harm; the degrees of resistance to attacks in these varieties of networks are rather low. To protect the confidentiality of the information shared in these networks, it has to be secured from malicious individuals and communal. Though Public Key Infrastructure (PKI) is a widely accepted scheme, it is much ill-suited for adoption in open and autonomous environments. Traditional approaches to security schemes cannot always be adopted in open and autonomous distributed environments; ensuring security in such open natured environments is a critical issue that is open for investigation. Recent researches have suggested an effective way to provide security by building 'Trust' among entities to sort out the most reliable entities to interact with. This essentially calls for quantifying levels of entity trust in a distributed environment and obtaining feedback to support the levels of trust entrusted on the entities. This paper proposes a decentralized transitive trust and data dispersal to secure data exchanges among entities (a few of which may be malicious) in ad-hoc networked environments.

Index Terms: Ad-hoc network, transitive trust model, IDA, trust based multi path approach.

1. INTRODUCTION

Ad-hoc networking is a fairly novel archetype having an edge of rapid deployment with relatively lower costs; this feature presents the avenue for commercial uses. Standard client-server approaches to data distribution fall behind when compared with ad-hoc networking. File sharing in ad-hoc networks have benefits in terms of increased availability, scalability and robustness. Equivalently these networks suffer from lack of accountability that stems directly from their open and anonymous nature. Evidently these networks open doors to maliciousness [6], [19], [20]. Conventional security approaches may be adopted in these environments [1], [9], [15] but they are rather ill suited; this stipulates the use of equivalent alternative approaches based on trust and / or reputation [4], [7], [12], [13], [18], [21] to secure routing of messages. The focus of the underlying problem is in determining secure and trusted paths [2], [3] for interactions and data exchanges. This essentially requires a suitable approach to enable data exchange over multiple paths (*n* paths) such that the original data can be recovered at the receiver despite failure in some of the transmitted paths (*n-k* paths).

In this paper, we present a data exchange method that integrates data dispersal of Information Dispersal Algorithm (IDA) with the concepts of transitive trust of intermediate nodes to propose a trust based multi path routing. First the messages are divided into *n* different parts using IDA. The *n* parts are then routed separately through different reliable paths based on the Eigen trust of the nodes intermediate that form the

* Department of Computer Science and Engineering, Amrita School of Engineering-Coimbatore Amrita Vishwa Vidyapeetham (University), Amrita Nagar PO 641112, Coimbatore, India, *Email: ck_shyamala@cb.amrita.edu*

** Department of Computer Science and Engineering, Amrita School of Engineering-Coimbatore Amrita Vishwa Vidyapeetham (University), Amrita Nagar PO 641112, Coimbatore, India, *Email: nivedaashok@gmail.com*

*** Department of Computer Science and Engineering, Amrita School of Engineering-Coimbatore Amrita Vishwa Vidyapeetham (University), Amrita Nagar PO 641112, Coimbatore, India, *Email: bhavya.narayanan123@gmail.com*

paths from source to destination. Our benefactions are aligned as follows: Section 2 details related studies in the literature for securing data exchanges in open and autonomous distributed environments. The proposed approach for dispersal based data exchange and selection of trusted and reliable paths for transmission is described in Section 3. The simulation explained in Section 4 approach validates the proposed data exchange scheme for threat models of individual and malicious communal nodes. Conclusion and future extensions of the work are discussed in Section 5.

2. RELATED WORKS

A multi-path strategy may be a wise choice for the exchange especially in infrastructure-less and improvised distributed environments when compared to single path exchange [14]. Here, the data can be fragmented into parts and each of the part can be sent through a unique path(node to node). One main challenge to securing data exchanges between source and destination in ad-hoc networks is their vulnerability to security attacks [5], [30]. Conventionally techniques like key based encryption systems, using certification authorities and digital signatures have been employed to ensure the security of the same. Hongru Wei and Chao Qi have discussed the possibilities securing the messages in an ad-hoc network while the message communication takes place over a single path [28]. Availability, confidentiality, integrity, authentication and non-repudiation are the important attributes that needs to be considered while securing the message exchange in an ad-hoc network and this has been effectively addressed by Lidong Zhou and Zygmunt J. Hass in their paper [31]. Further, the widely used and proven digital signature defense is ineffective against attacks from compromised and malicious entities.

In the light of the above discussion, it is necessary that the data exchange in ad-hoc network must be supported by mechanisms that overcome the vulnerability of the network to security attacks, the frequently changing unstable network and the short comings of using digital signature and certification authorities. There is a scope to investigate the use of trust based multi path routing in securing the message exchange between the source and destination in ad hoc network. Trust and reputation models are not only confined to ad hoc networks but also find applications in P2P networks, online shopping and storage and retrieval [8], [11], [22], [23], [24], [26], [27], [29]. Comprehending applications of trust and /or reputation in managing open and autonomous distributed environments and attempts to standardize the same has been of interest of research in [7], [8], [10], [16], [17], [21]. Research in [13] presents a reputation system that employs the concepts of local and global scores with minimized message complexities. Security of message in mobile Ad-hoc networks using the multi path routing approach on the basis of trust is in focus in [20]. An ad-hoc network message routing method using the notion of multi path routing and node trustworthiness includes message partitioning and encryption. The message parts are separately routed using different paths, based on trustworthiness, through Dynamic Source Routing (DSR) protocol.

We in this paper present a trust based multi path approach to secure the data exchange from one node to other by using Information Dispersal Algorithm (IDA) and Eigen trust. The simulation results confirm the proposed data exchange scheme for threat models of individual and malicious communal nodes.

3. PROPOSED MODEL

3.1. Secure message exchange

Message security is provided in the proposed scheme using IDA. The algorithm encodes a message '*m*' into '*n*' components such that any '*k*' components out of those '*n*' components are enough to reconstruct the original message. IDA provides a confidentiality level of *k*-1 and a fault tolerance of *n*-*k* [1,19 ,21]. The pseudo code of IDA in Figure 1 illustrates fragmentation of original data into n parts and reconstruction of the original data from the fragment parts.

Fragmentation (*n*, *k*, *F*)

$F = b_1, b_2 \ldots b_N$

1: $w \leftarrow [N/k]$
2: Initialize kxw matrix, D
3: Initialize $nx\,k$ matrix, A
4: position $\leftarrow 1$
5: for $i \leftarrow 1$ to k do
6: for $j \leftarrow 1$ to w do
7: if position £ N then
8: $D_{ij} \leftarrow b_{position}$
9: else
10: $D_{ij} \leftarrow 0$
11: end if
12: position $\leftarrow$ position + 1
13: end for
14: end for
15: for $i \leftarrow 1$ to n do
16: for $j \leftarrow 1$ to k do
17: $A_{ij} \leftarrow \alpha^{j-1}$
18: end for
19: end for
20: $C \leftarrow$ Matrix Multiplication (A, D)
21: Initialize share $_i$, $i = 1 \ldots n$
22: for $i \leftarrow 1$ to n do
23: for $j \leftarrow 1$ to w do
24: share $_i[j] \leftarrow C_{ij}$
25: $j \leftarrow j + 1$
26: end for
27: end for
28: return share$_1$, …share$_n$

Reconstruct(share$_1$, …share$_n$)

share$_i$= < $C_{i1} \ldots C_{iw}$,α_i >

1: Initialize $k\,x\,w$ matrix, C'
2: Initialize $k\,x\,k$ matrix, A'
3: for $i \leftarrow 1$ to k do
4: for $j \leftarrow 1$ to w do
5: $C_{ij}' \leftarrow C_{ij}$
6: end for
7: end for
8: for $i \leftarrow 1$ to k do
9: for $j \leftarrow 1$ to k do
10: $A_{ij}' \leftarrow \alpha^{j-1}$
11: end for
12: end for
13: $A_{inv}' \leftarrow$ Inverse (A')
14: $D \leftarrow$ Matrix Multiplication (A_{inv}', C')
15: position $\leftarrow 1$
16: for $i \leftarrow 1$ to k do
17: for $j \leftarrow 1$ to w do
18: $F_{position} \leftarrow D_{ij}$
19: position $\leftarrow$ position + 1
20: end for
21: end for
22: return F

Figure 1: IDA –Data Fragmentation and Reconstruction

3.2. Trust based multipath selection for data exchange

Figure 2 explains the multipath selection using Eigen Trust. Each fragment is routed through different intermediate nodes chosen based on Eigen trust iteratively to reach the destination.

3.2.1. Eigen Trust Model

The Eigen Trust model in [16] has been adopted by us to estimate and identify the intermediate trusted nodes and thereby the trust worthy paths for data exchange. The global trust vector is used to quantify

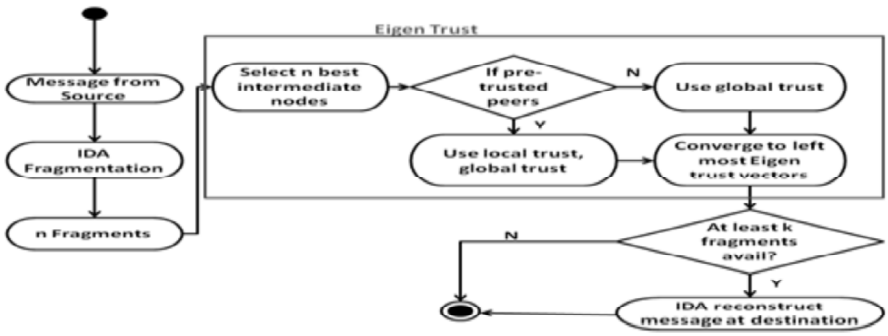

Figure 2:Activity Diagram

the trust ratings which the entire system places on a particular node while the local trust rating is used to quantify the trust ratings which each node places on the other based on its previous direct interaction. Let agr (u, v) be the count of agreeable transactions node u has had with node v (similarly, unagr (u, v)). Then, the local trust score A_{uv} is defined as the difference between agreeable and unagreable transactions as follows:

$$A_{uv} = agr\ (u, v) - unagr\ (u, v) \tag{1}$$

The local trust value is normalized. This is done as a corrective measure in retaliation to any feedback skewing mechanisms employed by malicious nodes. The normalized local trust ratings always lies in the interval [0, 1] and can be given as:

$$B_{uv} = \frac{\max(A_{uv}, 0)}{\sum v\ \max(A_{uv}, 0)} \qquad if \sum u \max(A_{uv}, 0) \neq 0$$

$$B_{uv} = P_v \qquad \text{otherwise} \tag{2}$$

where p is the pre-trusted node. If P nodes are known to be pre-trusted, then the pre-trust value $p_u = 1/|P|$ if $u \in P$ and $p_u = 0$ otherwise. Thus, if node is not aware of any other nodes, or does not believe any node, it will decide to trust the endorsed nodes termed as 'pre-trusted'. The normalized local trust needs to be aggregated. This has to be done because the local trust values are weighted by the global trust values. The aggregation of normalized local trust values (lt) that node 'u' places on node 'k' on the basis of reputation that k's immediate neighbours has on 'k' is computed as:

$$lt_{uk} = \sum u B_{uv} B_{vk} \tag{3}$$

Let B be the matrix $|B_{uv}|$ and lt_v be the vector comprising the values lt_{uk} then

$$lt = B_T b_u \tag{4}$$

To get a total view of the network, node 'u' can advance with n iterations by asking its neighbour's neighbour recommendations about nodes. If n is big enough, the t_u trust vector will coincide to the left principal Eigen vector of B.

To break down the malicious communal, we have used endorsed nodes (the pre-trusted ones) to enhance the performance of our system. The presence of endorsed nodes makes certain that the normal nodes move towards the pre-trusted value. Therefore, the updated global trust value is formulated as:

$$lt^{(k+1)} = (1 - a)\ (B^T)\ (lt^{(k)}) + (a)\ (p) \tag{5}$$

where 'a' is an empirical constant smaller than 1 and $lt^{(0)} = p$

3.3. Secure message exchange using trust based multipath routing

A secure transaction, is the passing of the data in parts (data fragments obtained from IDA) through a sequenced set of trusted intermediate nodes to reach the destination. On the onset it is required that the source nodes identify the required set of n nodes. It then send s a unique data fragment to each one of the n nodes. Each of these n nodes consequently identifies the next immediate trusted intermediary to pass on their data fragments. These result in a set of n reliable/trusted paths from source to destination, facilitating a trust based multipath routing. The destination node may recover the original data with a minimum of k of the data fragments from any k of the paths. Nodes along the paths evaluate their immediate intermediate node based on the service that they have been provided with. Figure 3 illustrates a high-level view for secure data exchange between a source and destination over reliable paths defined by trusted intermediate nodes.

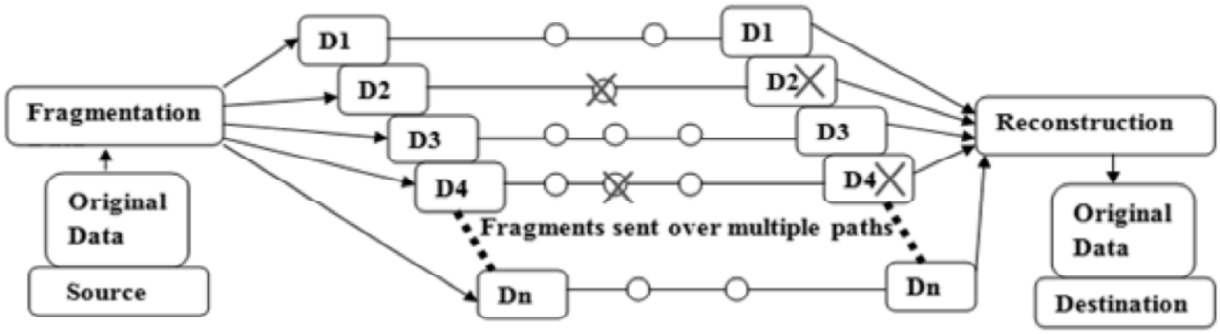

Figure 3: Secure message exchange over reliable paths

4. SIMULATION AND RESULTS

A typical ad-hoc network is considered for simulation. The simulation runs through a series of queries between the nodes wherein the nodes either request the query or respond to the incoming query. Based on the feedback given on a complete transaction, updated global trust value is computed for the nodes.

The experimental set up includes a collection of *pre trusted nodes* (anonymous nodes that keep up the trust ratings of the system), *regular nodes* (normal nodes, that take part in the network to upload files) and *malicious nodes* (hostile nodes [19], that take part in the network to weaken its execution).The scheme's performance is demonstrated for threat models A-malicious nodes and B-malicious communal. The simulations were performed under varied percentage of hostile nodes in the network. We have considered the simulations run in cases where we have included the trust model and in those which have no trust model. In the absence of a trust and reputation system in the network, the malicious nodes which are present in the network end up receiving a greater number of parts of the message which finally results in an increased number of inauthentic uploads. The results of the simulations prove that the proposed secure trust based multipath data exchange effectively reduces the number of corrupt data exchanges and uploads. Also it reflects the efficiency of the model in suitably selecting the reliable trusted paths and subverting the malicious and communal malicious nodes. Ratios in the tables 2 and 3 show an increase in trend when compared to table one, indicating the success of the proposed scheme and also visualized in corresponding bar charts.

I. Threat Model A – NAÏVE (Individual Malicious Nodes):

Malicious nodes often provide polluted data when chosen as an intermediate node or as an upload source. The proposed scheme prevents malicious nodes from subverting the system; malicious nodes are rarely chosen as an intermediate node or as source of upload because of their lower trust value. This lowers the number of corrupt data transferred from malicious nodes. Figure 4 and 5 illustrate the results of the simulation

Table 1
Nil Trust

Ratio of % of malicious nodes to % of inauthentic downloads	*Ratio of valid transaction to dishonest feedback*
0.8	11.29
1.24	5.54
1.623	3.166
1.44	1.066

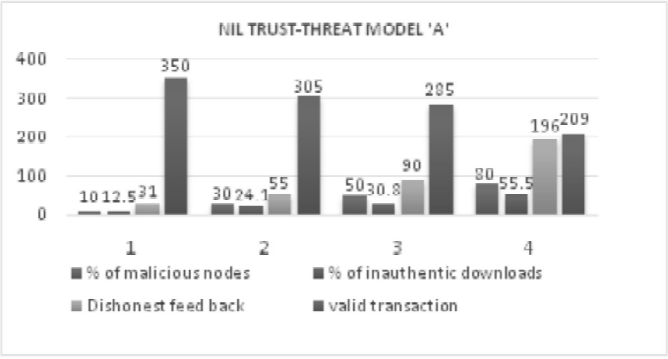

Figure 4: Case of NIL Trust – Threat model A

Table 2
Naive Eigen Trust

Ratio of % of malicious nodes to % of inauthentic downloads	*Ratio of valid transaction to dishonest feedback*
2.9	12.67
5	6.14
8.9	3.90
14.81	1.14

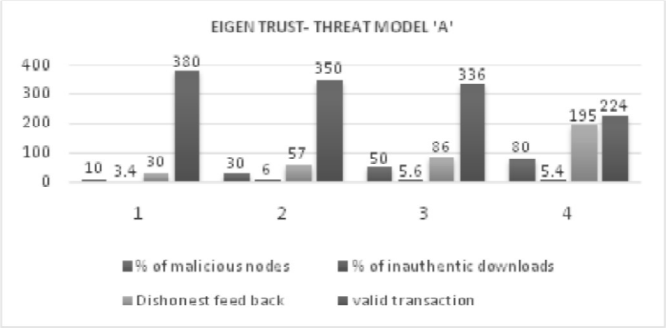

Figure 5: Case of Eigen Trust– Threat model A

for varied percentage of malicious nodes in the network for Threat Model A –Naïve with no trust and Threat model A-Naïve with Eigen trust respectively. It is observed that there is a notable reduction in the number of corrupt data exchange in the network, when the proposed scheme is adopted.

II. Threat Model B – COOPERATIVE (Malicious Communal):

A malicious communal is formed when group of malicious nodes get together and mutually increase their trust values. The proposed approach uses pre-trusted nodes to prevent this unfavorable experience. From Figure 6, it is observed that there is a notable reduction in the number of corrupt data exchanges in the network with the application of the proposed approach.

Table 3
Collaborative Eigen Trust

Ratio of % of malicious nodes to % of inauthentic downloads	*Ratio of valid transaction to dishonest feedback*
2.86	16.73
6.122	5.48
14.71	2.57
14.81	1.22

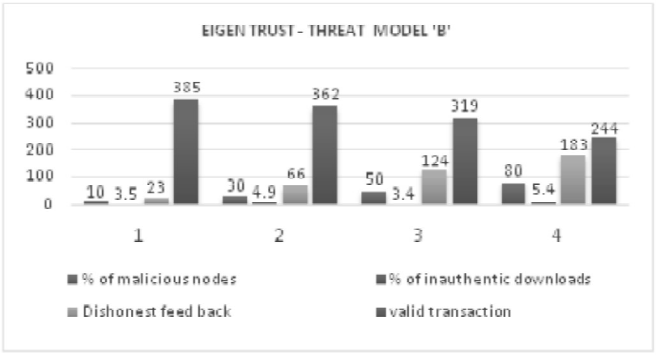

Figure 6: Case of Eigen Trust– Threat model B

5. CONCLUSION

We have presented a model that ensures security of data in exchange from a source to destination using IDA. Further, the transitive trust approach in the calculation of global trust score, using pre-trusted nodes, isolates the communal malicious nodes from the network. The computation of trust takes every node's recommendation into account; how-ever the impact of each recommendation varies. The simulation results bring out the proposed scheme ability to mitigate both individual and communal maliciousness. The proposed work can be extended to allow change user models mid-trace [25], and insert new files into the network are all future considerations. There is scope to enhance the feedback mechanism; entry of additional feedbacks may allow for more powerful methods of trust computation. Trust reputation modeling can also be done using self-organization as presented in [11]. It could be opted for as an effective alternative as it considers recommendation factors in addition to trust and reputation.

References

[1] Abdallah, Aisha, and Mazleena Salleh. "Analysis and Comparison the Security and Performance of Secret Sharing Schemes." *Asian Journal of Information Technology* 14.2 : 74-83, 2015.

[2] Abdul-Rahman, A., and S. Hailes. "A Distributed Trust Model In New Security Paradigma." *Workshop*. 1997.

[3] Abdul-Rahman, Alfarez, and Stephen Hailes. "Supporting trust in virtual communities." *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*. IEEE, 2000.

[4] Aberer, Karl, and Zoran Despotovic. "Managing trust in a peer-2-peer information system." *Proceedings of the tenth international conference on Information and knowledge management*. ACM, 2001.

[5] Ahmeda, Shubat S. "ID-based and threshold security scheme for ad hoc network." *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*. IEEE, 2011.

[6] Ahmed, Adnan, et al. "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks." *Frontiers of Computer Science* 9.2 (2015): 280-296.

[7] Almenárez, Florina, et al. "PTM: A pervasive trust management model for dynamic open environments." *First Workshop on Pervasive Security, Privacy and Trust PSPT*. Vol. 4. 2004.

[8] Beth, Thomas, Malte Borcherding, and Birgit Klein. *Valuation of trust in open networks*. Springer Berlin Heidelberg, 1994.

[9] Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol." *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2002.

[10] Buchegger, Sonja, and Jean-Yves Le Boudec. "A robust reputation system for peer-to-peer and mobile ad-hoc networks." *P2PEcon 2004*. No. LCA-CONF-2004-009. 2004.

[11] Can, Ahmet Burak, and Bharat Bhargava. "Sort: A self-organizing trust model for peer-to-peer systems." *Dependable and Secure Computing, IEEE Transactions on* 10.1 (2013): 14-27.

[12] Gambetta, Diego. "Can we trust trust." *Trust: Making and breaking cooperative relations* 13 (2000): 213-237.

[13] Kamvar, Sepandar D., Mario T. Schlosser, and Hector Garcia-Molina. "The eigentrust algorithm for reputation management in p2p networks." *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003.

[14] Khan, Muhammad Saleem, et al. "Adaptive Trust Threshold Strategy for Misbehaving Node Detection and Isolation." *Trustcom/BigDataSE/ISPA, 2015 IEEE*. Vol. 1. IEEE, 2015.

[15] Mariappan, Ramasamy, and Sangameswaran Mohan. "Re-Pro Routing Protocol with trust based security for Broadcasting in Mobile Ad hoc Network." *Advanced Computing (ICoAC), 2011 Third International Conference on*. IEEE, 2011.

[16] Mármol, Félix Gómez, and Gregorio Martínez Pérez. "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems." *Computer Standards & Interfaces* 32.4 (2010): 185-196.

[17] Marsh, Stephen Paul. "Formalising trust as a computational concept." (1994).

[18] Marti, Sergio, and Hector Garcia-Molina. "Taxonomy of trust: Categorizing P2P reputation systems." *Computer Networks* 50.4 (2006): 472-484.

[19] Martin, Keith M. "Challenging the adversary model in secret sharing schemes." *Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts* (2008): 45-63.

[20] Narula, Prayag, et al. "Message security in mobile ad-hoc networks: Using trust-based multi-path routing approach." *Computer Engineering & Systems, 2007. ICCES'07. International Conference on*. IEEE, 2007.

[21] Parakh, Abhishek. *New Information Dispersal Techniques for Trustworthy Computing*. Diss. Oklahoma State University, 2011.

[22] Resnick, Paul, et al. "Reputation systems." *Communications of the ACM* 43.12 (2000): 45-48.

[23] Shyamala, C. K., & Aiswarya, P. L. Design of Fair Testimony in Reputation Systems. *International Journal of Applied Engineering Research*, 9(23), 2014.

[24] Shyamala, Coimbatore K., and Tattamangalam R. Padmanabhan. "A Trust–Reputation Model Offering Data Retrievability and Correctness in Distributed Storages." *International Journal of Computers and Applications* 36.2 (2014): 56-63.

[25] Srivatsa, Mudhakar, Li Xiong, and Ling Liu. "TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks." *Proceedings of the 14th international conference on World Wide Web*. ACM, 2005.

[26] Wang, Wei, Guosun Zeng, and Lulai Yuan. "Ant-based reputation evidence distribution in P2P networks." *Grid and Cooperative Computing, 2006. GCC 2006. Fifth International Conference*. IEEE, 2006.

[27] Wang, Yong, et al. "Bayesian network based trust management." *Autonomic and Trusted Computing*. Springer Berlin Heidelberg, 2006. 246-257.

[28] Wei, Hongru, and Chao Qi. "A new security mode based identity encryption in Ad Hoc network." *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*. IEEE, 2011.

[29] Xiong, Li, and Ling Liu. "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities." *Knowledge and Data Engineering, IEEE Transactions on* 16.7 (2004): 843-857.

[30] Zhang, Guanghua, et al. "Using Trust to Establish a Secure Routing Model in Cognitive Radio Network." *PloS one* 10.9 (2015): e0139326.

[31] Zhou, Lidong, and Zygmunt J. Haas. "Securing ad hoc networks." *Network, IEEE* 13.6 (1999): 24-30.