Enhancing the security and routing reliability for achieving efficient data transmission in mobile Ad Hoc Networks

GATETE MARCEL

Research Scholar,
School of Comp. Sciences & Applications
Periyar Maniammai University, Thanjavur, TN, India
E-mail: gtmrcln@gmail.com

Dr. N. Vetrivelan

Director,
Centre for University Industry Interaction,
Periyar Maniammai University, Thanjavur, TN, India
E-mail: nvetri@yahoo.com

Abstract- A Mobile Ad hoc Network is a wireless network in which a central management scheme is not available; this causes nodes to dynamically self-organize each one playing both router and node's roles. Compared to the other types of wireless networks, the infractureless nature of this type of network makes it provide various advantages with some numerous problems of course. One problematical approach toward routing in MANET is the security issues, which, combined with reliable data transfer problems make some MANET's users unsatisfied. This security problem is explained in the fact that as participating nodes regularly communicate and exchange information; there must be a level of trust between them. Some weak protocols are designed in such a way nodes randomly exchange messages without any control due to the lack of trust management mechanisms which may be required to prevent such unsecure information exchanges; thus opening a way to unwanted malicious nodes and intruders compromising the security in MANET, and in turn, resulting in unreliable data transmission. This paper conducts a performance evaluation of various security-aware algorithms based on trustworthy schemes namely trust evaluation with direct observation and trust evaluation with indirect observation. These two schemes are evaluated against the existing one while varying the routing metrics available for MANETs; throughput, hacked packet ratio, end-to-end delay ratio, and the overall trust valuation metrics. This performance evaluation is conducted for the Optimized Link State Routing Protocol version2 (OLSR v2), the successor and enhancement of OLSR v1. It has been chosen thanks to its capability to efficiently extend MANET's neighborhood discovering process, a feature which makes it easy to detect malicious neighbor and distant nodes in the network. The simulations are carried out using NS-2 while varying the number of nodes, the outcomes show that the trust evaluation with indirect observation approach outperforms the other schemes; the direct observation scheme mediumly performs while the existing one is always worsened except with the end-to-end delay parameter.

Keywords: MANETS, Reliable transmission, Security, Trust Management, and Simulation.

I. INTRODUCTION

Mobile networking [9] involves various mobile nodes communicating and exchanging information instantaneously. MANET's participating nodes must be extremely cooperative in transferring data and routing messages without a rigorous central manager, this ends up in an unexpected opening to many new attacks. For instance, an intruder may act as a neighbor to the legitimate node and both start exchanging messages, this is a malicious event which adversely affects the whole network's performance.

Various trust management schemes have been developed with a special purpose of achieving highly reliable data transmissions such as secure routing, authentication, intrusion detection, and access control (authorization). Despite those efforts, some protocols are not designed with such features resulting in various security issues being posed. For this end, this paper provides a rigorous solution to this problem by enhancing the security and reliability of data transmission in mobile Ad hoc Networks by taking into consideration both the node's social trust and QoS trust properties thanks the trust evaluation with indirect and direct observations mechanisms evaluated against the existing scheme. These two approaches in combination with throughput, hacked packet ratio, average end-to-end delay, and the mean trust value routing metrics; we assess the accuracy of these security mechanisms for the OLSR V2 protocol.

II. BACKGROUND OF THE STUDY

C. Adjih et al. [1] conducted their research in MANETs, especially about OLSR's security issues. For this, they proposed a detailed architecture containing various securing mechanisms for this protocol which was being implemented. Various attacks were highly prevented from spreading throughout the network by this architecture, they also provided some details about the protocols used along with their relevant algorithms and mechanisms.

S. Bu et al. [2] combined two effective approaches in securing Mobile Ad hoc Networks namely continuous user authentication and intrusion detection systems (IDS). They stated that these combined security mechanisms provide an optimal security design as a solution to security requirements and resource constraints in MANETs. To this end, they formulated the problem as a partially Observable Markov Decision Process (POMDP) multi-armed bandit problem with optimal policy being able to be chosen using Gittins indices. The outcomes of their experimentation using simulation revealed that their proposed distributed scheme was effective with a very high performance. They finally stated that in the future, they planned to consider more node’s states i.e. mobility and wireless; their currently proposed scheme would be also implemented in a real testbed.

Zouridaki et al. [3], Due to the secure and reliable packet delivery related problem often faced by MANET’s users, proposed a robust cooperative trust establishment scheme aiming at improving the reliability of packet delivery ratio for this type of wireless network. This scheme efficiently performed very well even in the presence of malicious nodes. With it, each node relies on the trustworthiness (first-hand and second-hand trust information obtained from of the other nodes). The first-hand trust information of a neighbor node is collected at the MAC layer via direct observation while for the non-neighbor node; this information is obtained via an acknowledgment packet sent as a reply of the successful reception of the transmitted packet. Here, the information sharing mechanism between nodes plays an important role as it accelerates the convergence of the trust establishment procedure. The simulation results revealed that this proposed scheme was very effective even in the presence of malicious nodes during the data transmission processes either with packet forwarding or trust propagation mechanisms.

F. Yunfang [4] stated that various trust management systems are necessary for an authorization decision to be made for a node to communicate with a stranger one. The first system is a policy-based approach with which authorization decisions are made according to the logical rules and verifiable properties in signed credentials. A second system is a reputation-based approach aiming at collecting, aggregating, and disseminating reputation among nodes. He again stated that those two approaches often face various challenges which inhibit them achieving their relevant objectives; the policy-based approach may face both the overhead caused by the proof of compliance on both the authorization and unavailability caused by the lack of evidence in making decision whereas the reputation-based approach’s objective achievements may be inhibited by whilst vagueness, complexity, and inaccurate characterization caused by the reputation evolution. He finally proposed that an integrated approach would enhance these trust mechanisms by integrating two notions into trust management processes such as the policy proof and reputation evolution which finally results in strong security enhancements, calculability, and the availability of security implications, thus designing a trust management framework incorporating trust.

A. Jayakumari et al. [12] in their paper developed a trust management scheme which enhances the security issues in Mobile Ad hoc Networks. They fixed two types of trust values for each node, values derived from both direct and indirect observers, based on which, a relevant decision was made concerning to whether a node would be selected for participating in the routing process or not. With this secure routing mechanism, they improved the routing security in MANETs resulting in an increased packet delivery ratio. In their conclusion, the stated that the main objective of their paper was to provide multiple perspectives on trust management model to various protocol designers, so, they proposed that future researchers should develop the trust management model taking into consideration the adaptation to the environmental dynamics, scalability, reliability, and reconfigurability attributes.

III. TRUST MECHANISMS DESCRIPTION

Trust mechanism has been used by various protocol designers as it provides different advantages to Mobile Ad hoc Networks. Those advantages are of a very big importance as there must be a trust relationship between participating nodes otherwise some intruders and malicious nodes would participate in exchanging information with other authentic nodes, an activity which should never be allowed during this type of wireless network’s operations.

Trust management approaches are one of the solutions available for the previous problem, in [13] it is defined as a collection of relationships linking various participating entities playing a major role in a given protocol. The previous collaboration of these entities provides a landmark for the future relationship establishment operations; in other words, if no previous relationship exists between two nodes, this may result in denying this new relationship as one of them may be an unauthenticated node even a malicious one. Here the degree of belief among those nodes is necessary to establish the current trust among them; low value means the trust relationship establishment may be further fading.

Sometimes the terms ‘trust’ and ‘trustworthiness’ may be used interchangeably but they are truly and slightly different as the trust’s level can takes two values i.e 0 for a complete node’s distrust and 1 for a complete trust while the trustworthiness may be the probability that the trustees will behave as it has been expected. When the level of trust is zero, the risk value gets higher while it gets lower with the increasing trust’s value. The risk always exists even when the trust’s value is 1. Generally trust is neither proportional nor inversely proportional to risk.

3.1. Trust types

One should classify trust into two categories namely context independent reliability trust and decision trust. These two types of trust concepts are used by nodes in MANET.

a) Context-independent reliability trust

Nicknamed “reliability trust”, this type of trust estimates the apparent trustworthiness made by another third node without taking into consideration of the situation the trustor might face by considering the potential risks. In short, reliability trust of a node is defined as the trust of another node regardless or independently of the context.

b) Decision trust

This type of trust relies on the situation where a given entity is relying on some other entity in seeking for security without worrying the negative consequences which would arise. Utility and risk attitude are two components usually dealt here. Similarly, in MANETs, if a given task requires high computational power, a node with this high power is regarded as trusted while a non-malicious node (i.e., honest) that has low computational power) is distrusted.

3.2. Trust features

For a social network, there exist three main properties of trust [namely transitivity, asymmetry, and personalization [14]. For example if a node ‘A’ truly trusts the node ‘B’, while ‘B’ trusts in turn the node ‘C’, this does not guarantee that the node ‘A’ trusts the node ‘C’; this indicates that ‘trust’ is not mathematically a perfect transitivity. For the transitivity to be valid a trust between two nodes for example to a new third node must exist and the trustor should have two types of trust i.e. trust the trusted node and trustee’s recommendation of the third party.

The relationship (trust) between an employer and employee is a perfect example of asymmetry property of trust as it does not occur identically in both directions, in MANET, a highly capable node may not trust nodes with lower capability while the latter ones may fully trust the former ones. Thirdly, people have different perspectives and opinions about the same trustworthiness evaluation of the same entity which makes trust a personal opinion, here a node’s choice of its own trustworthiness criteria may differ from others’.

3.3. Trust management for MANETs

The trust management is a part of risk management process aiming at authenticating entities under uncertainty, and decision-making on cooperation with stranger entities [15]. The trust management process is composed by the following stages: trust establishment (trust evidence collection, trust generation, trust distribution, trust discovery, and evaluation of trust evidence), trust update, and trust revocation.

Two type of trust can be achieved in two ways: trust from direct observation and trust from indirect observation.

3.3.1. Trust with direct observation

With the direct observation from an observer node, the trust value is derived using Bayesian inference [16]. With this direct observation technique, we detect a malicious behavior: hacked packets (stolen and modified packets). Here, we tend to assume that every observer will catch packets forwarded by the observed node and compare them with the original packets, so the observer will determine the malicious behaviors of the ascertained node. Therefore, it will calculate trust values of this node using Bayesian interference; a framework aiming at estimating the unknown probability with the help of an observation procedure.

3.3.2. Trust with indirect observation

An indirect observation also called secondhand information is obtained from neighbor nodes of the observer; the trust value then results using the Dempster-Shafer theory [16], a mathematical theory of evidence providing a numerical measurement of degrees of belief about a proposition from multiple sources. This technique is also very important in assessing the trust value of the observed node as it plays a major role of testimony from neighbor nodes which is very helpful in judging the trustworthiness of the observed node by evaluating the trust value of the observed node assigning two security states to a node, i.e., {trustworthy, untrustworthy}. A node can be judged hostile or not based on this complementary information obtained from neighbor nodes; this may reduce the bias from an observer node where this observed node can be benign to the observer but very malicious to another.

3.4. Mathematical evaluations and algorithms of direct and indirect observations

We use the mathematical assumptions and algorithms previously used in [16] for calculating trust values of each node located along the path which a sender should forward packets through.

IV. EXPERIMENTATION AND RESULTS

The same research previously done in [16] focused on OLSR v2, a proactive routing protocol which efficiently enhances neighborhood discovering process between nodes which make it an excellent protocol in detecting malicious neighbor and distant nodes in the network. The experiments were previously done applying only one routing metric parameter; packet delivery ratio (PDR), which is not much enough in exhibiting the overall outperformance of both direct and indirect observations schemes when compared to the existing one.

In this paper, with the same protocol and approaches, we conduct the same performance evaluation by changing and increasing the number of routing metrics namely throughput, the number of hacked packets, end-to-end delay, and the mean trust values obtained from both direct and indirect observations trust values for each and every the network' density.

4.1. Routing metrics

There are four performance metrics considered in the simulations:

4.1.1. Throughput

Throughput or network throughput is the rate of successful message delivery over a communication channel. In ns-2, it is defined as the total number of packets delivered over the total simulation time.

4.1.2. Hacked packet fraction

Hacked packets fraction is the total number of packets modified or stolen by malicious nodes. This fraction is obtained by conducting the performance evaluation with direct and indirect observation schemes.

4.1.3. Average end-to-end delay

End-to-end delay ratio is the average time necessary for a packet to reach the destination. It may be caused by many factors such as router discovery cycle and queuing process used during data packet transmission. Only data packets that have been successfully delivered to the destination are counted. The performance of the protocol is determined by the value of end-to-end delay; the lower ratio means the higher is the performance of the protocol.

End-to-end delay ratio=∑ (packet-arrive time – packet-send time) / ∑ Number of connections

4.1.4. Average trust value

The average trust value is the mean rate obtained from trust values of both indirect and direct observation schemes.

4.2. Simulation parameter values

Table 1: Network parameters

Number of nodes	0,5,10,15,20,25,30
Topology Size	500 x 500 m
Simulation Time	700 seconds
Packet Size	512 byte
Packet Rate	8 packets/second
Traffic Type	Variable Bit Rate (VBR)
Mobility Model	Random Way Point (RWP) Model
Channel Type	Wireless Channel
Antenna Model	Omni-Directional Antenna
Radio Propagation Model	Two-RayGround model
Mac Layer Protocol	IEEE 802.11
Maximum queue's length	50
Protocol	OLSR V.2

4.3. Results and discussion

4.3.1. Throughput

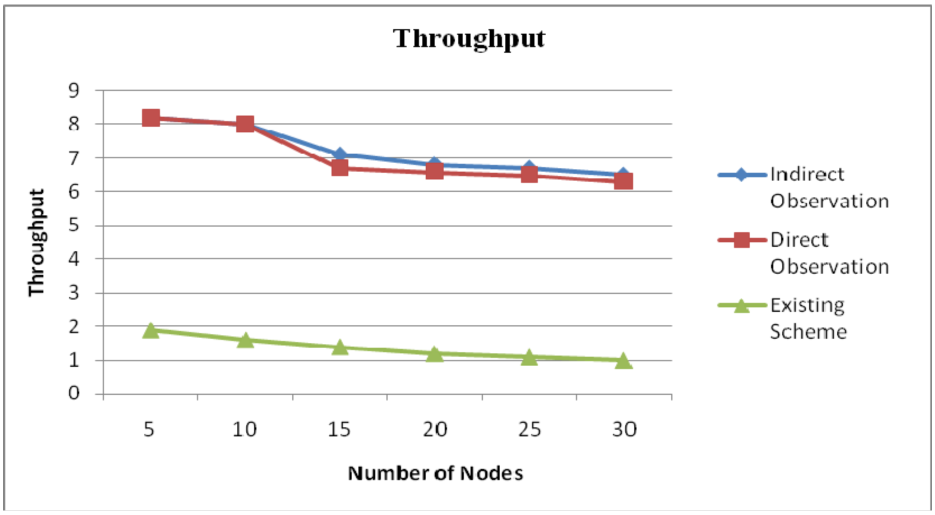

Figure 1: Number of nodes vs throughput

As we look at figure 1, taking into account the throughput metric for low-, medium-, and high-dense networks, the indirect scheme performs better than the others but with a minor differential to the direct observation, this is due to the fact that the indirect observation provides accurate results as the information about the malicious nodes is collected by different neighbor nodes compared to the one collected by a single observer node for direct observation evaluation scheme, this increases the throughput ratio as the data packets' transmission is more secure because the malicious node which would inhibit packets to successfully reach the destination have been denied for participating in the messages exchange processes. The existing scheme always performs badly for lowly and highly dense networks. One interesting observation for all the three schemes, the throughputs degrade inversely proportional to the increasing number of nodes.

4.3.2. Hacked packets ratio

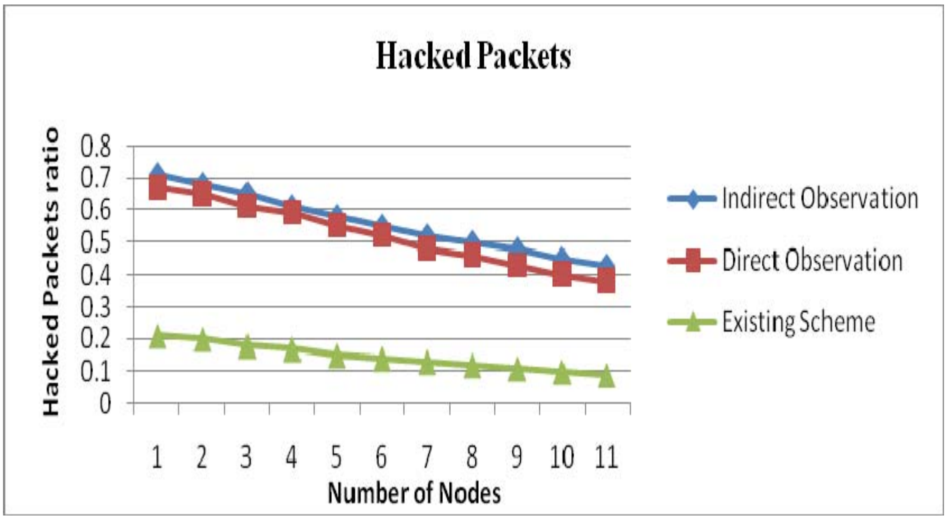

Figure 2: Number of nodes vs Hacked packets

Considering the hacked packets measurement, the existing scheme always performs worse for the overall simulation time with a small decreasing number of hacked packets ratio. Both indirect and direct observations scheme performs well as their relevant hacked packets' ratios continuously decrease as we increase the number of nodes. The indirect observation scheme again outperforms, this is a good indication that while in general more packets are hacked with continuously increasing number of nodes, here the stolen and modified packets ratio decreases as the network's density augments this achievement is possible thanks to as the number of nodes increases, this also augments the number of neighbor nodes which will play a very important role in discovering malicious nodes and intruders in the network which are immediately prohibited from participation into the network's message exchanges. Thanks to this features, the number of stolen and modified packets is minimized.

4.3.3. End-to-end delay

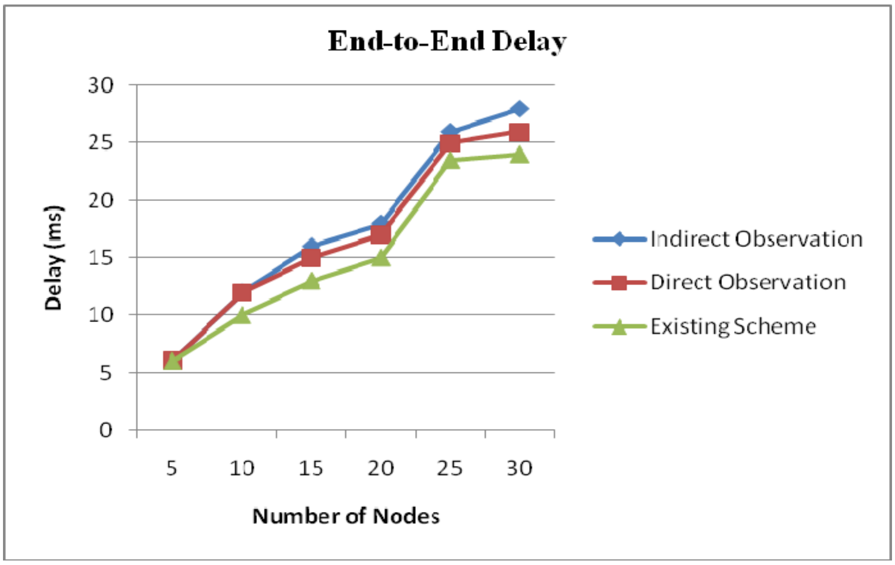

Figure 3: Number of nodes vs End-to-End Delay

Concerning the end-to-end delay parameter, the delay ration obtained with the indirect observation scheme is very high compared to the others but with a minor difference. Two interesting observation with this evaluation is that when the number of nodes is five, all the schemes have a very low delay (6 ms) which starts increasing as we increase the number of nodes. Another important revelation of this simulation experiments is that the existing scheme is performing well compared to the others as it maintains a lower delay ratio for the overall simulation time, the main cause of this behavior is that for both direct and indirect schemes the sender classifies some intermediate nodes as suspect to be malicious or intruders, those nodes may be along the path the packets should pass through, an end-to-end delay occurs as the protocol has to choose alternative routes to pass packets through which takes some amount of time.

4.3.4. Average trust value

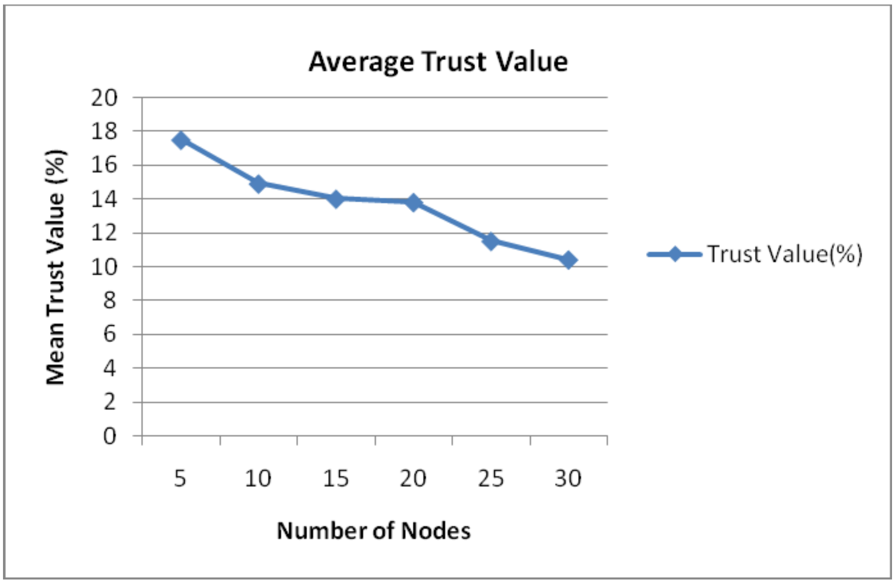

Figure 4: Number of nodes vs Average Trust value

Figure 4 exhibits the mean values obtained from both direct and indirect schemes. As we can see on the figure, when the number of nodes augments, the trust values' mean proportionally decreases. The main reason of this behavior is that the number of intruders and malicious nodes increases when the network's size enlarges. This reveals why those security-aware schemes are required for achieving an efficient transmission throughout the whole network as they detect malicious nodes compromise very much the network's operations.

V. CONCLUSION

This paper mainly aims at enhancing the security and reliability of data transmission in Mobile Ad hoc Networks which was achieved by evaluating the performance of three security-aware algorithms based on the trustworthy feature; Trust with direct observation, trust with indirect observation, and the existing scheme. On the contrary of the previous research done on the same schemes using a single evaluating metric, we conducted our experiments with an augmented number of parameters; four performance metrics namely throughput, hacked packets fraction, end-to-end delay ratio, and the overall mean trust values. This helped us so much in evaluating the strength and weaknesses of those trust valuation scheme for various scenarios which was never done before. The overall observation for all those three approaches; the indirect scheme almost worked well for all the cases studied as it increased the throughput with a minimized number of hacked packets but worked worse when we evaluated it with the end-to-end delay parameter where its ratio was maintained high during the overall simulation time. Concerning the direct observation scheme, this approach almost worked mediumly in all the cases studied with a minor difference to the indirect scheme when we applied the throughput and hacked packet ratio but while with end-to-end delay evaluation parameter it performed better than the indirect observation scheme, but this time the existing scheme outperformed them all. An overall observation is that the performance of all these three schemes almost weaknesses as the number of nodes increases. We propose that a future experimentation is carried out with a real testbed for real-life outcomes about these security schemes which are very important in enhancing the performance of the overall Mobile Ad Hoc Networks especially for routing related matters.

VI. REFERENCE

[1] C. Adjih, D. Raffo, and P. Muhlethaler, “Attacks against OLSR: distributed key management for security, ” in Proc. 2nd OLSR Workshop, (Domaine de Voluceau, France), Dec. 2005.

[2] S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, “Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks”, IEEE Trans. Veh. Tech., vol. 60, pp. 1025 –1036, Mar. 2011.

[3] Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, “Robust Cooperative Trust Establishment for MANETs,” Proc. 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, 30 Oct. 2006, pp. 23-34.

[4] F. Yunfang, “Adaptive Trust Management in MANETs,” Proc. 2007 Int’l Conf. on Computational Intelligence and Security, Harbin, China, 15-19 Dec. 2007, pp. 804-808.

[5] Theodorakopoulos 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, Feb. 2006, pp. 318-328.

[6] Josang and S. LoPresti, “Analyzing the Relationship between Risk and Trust,” Proc. 2nd Int’l Conf. Trust Management (iTrust’04), LNCS, Springer-Verlag, 2004, pp. 135-145.

[7] Yanchao Zhang, Member, Wei Liu, Wenjing Lou, Member and Yuguang Fang, ― Senior Member, Securing Mobile AdHoc Networks with Certificateless Public Keys‖. IEEE transactions on dependable.

[8] J. Li, R. Li, and J. Kato, “Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks,” IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[9] J. Loo, J. Lloret, and J. H. Ortiz, Mobile Ad Hoc Networks: Current Status and Future Trends. CRC Press, 2011.

[10] C. Adjih, D. Raffo, and P. Muhlethaler, “Attacks against OLSR: distributed key management for security,” in Proc. 2nd OLSRWorkshop, (Domaine de Voluceau, France), Dec. 2005.

[11] F. R. Yu, H. Tang, S. Bu, and D. Zheng, “Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks,” EURASIP J. Wireless Commun. Networking, vol. 2013, pp. 188–190, July 2013.

[12] A.Jayakumari, M.Sakthivel, “Trust Management Model Observation towards Security Enhancements and QoS in MANET’s”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015

[13] L. Eschenauer, V. D. Gligor, and J. Baras, “On Trust Establishment in Mobile Ad Hoc Networks,” Proc. 10th Int’l Security Protocols Workshop, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.

[14] J. Golbeck, “Computing with Trust: Definition, Properties, and Algorithms,” Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks, Baltimore, MD, 28 Aug. – 1 Sep. 2006, pp. 1-7.

[15] Solhaug, D. Elgesem, and K. Stolen, “Why Trust is not proportional to Risk?” Proc. 2nd Int’l Conf. on Availability, Reliability, and Security (ARES’07), 10-13 April 2007, Vienna, Austria, pp. 11-18.

[16] Thamayanthi.M et al., “Unified Trust Management Scheme that Enhances Security in MANET Using Uncertain Reasoning”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015