Collaborative Trust Model for Reactive Routing Protocols of MANETs

[1]Dr. A Sudhir Babu, [2]Mr. B Narasimha Swamy, [3]Dr. V. Srinivasa Rao

[1,3]Professor, [2]Sr. Asst. Professor
[1, 2]Department of Computer Science and Engineering,
PVP Siddhartha Institute of Technology, Vijayawada, India
[3]Department of Computer Science and Engineering,
V R Siddhartha Engineering College, Vijayawada, India

***Abstract*—Communication and network protocol designers consider trust as an important factor in order to optimize the system performance indicators.Embedding of trust is necessary among participating nodes within a network to achieve the better performance. The trust is defined by 'a set of relationships among nodes that participate in an event'. These relationshipsdepend upon the facts generated by the earlier communication between entities within a protocol. Trust accumulatesin the nodes, when the exchanges have been reliable to the protocol. The trust isthe degree of faith about the behavior of other entities. The trust level is specified as the faith probability ranging from 0 (complete distrust) to 1 (complete trust).In this paper, a trust model is presented without requirement of third party trust.The established trust by trust model is maintained trust in the MANET. The trust is established in MANET without any superfluous assumptions, requirements and cryptographic mechanisms.The existing routing protocols establish the required trust level by presenting trusted third party. Trusted third party can be realized by adapting cryptographic mechanisms in the routing process between nodes. The proposed trust model is used to acquire required trust level even in the absence of third trusted party**

***IndexTerms*—MANET, Trust Agent, Reputation Agent, Trust Mixer.**

I. INTRODUCTION

The trust development between nodes is very much needed to compute the dependability of other nodes.The endurance of a wireless sensor network is relatively depends on the supportive and trust environment of its hops.The proposed trust model is represented by three layers of trust and shown in Figure 1.

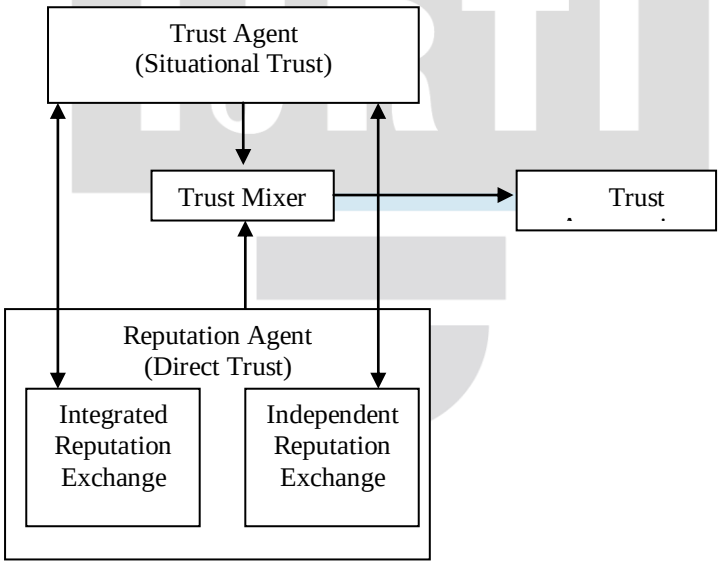

Figure 1: Structure of the Trust Model

Situational trust is an entity, which can be placed in another entity depending upon previous transactions. The trust agent weighs up the good factors in all situations by considering the utility of prior knowledge available.In layer 1, the trust agent resides at each node of the network. The trust agent refines the trust values, which are derived by a node. In layer 2, the reputation agent accumulates the trust value of each node by transmitting Route_Req and Route_Rep packets. In this layer, the direct trust

relationships are established between neighborhood nodes. In layer 3, the trust mixer combines the trust agent and reputation agent. The outcome of the trust mixer is treated as trust aggregation[9].

To reduce the complexity of trust model, the trust establishment and development process is devised by a variable called weight [2]. The weight is an evaluating factor, which is important to derive and compute trust level.

II. Reputation Agent

The majority of events such as route requests, route replies and acknowledgements etc. between adjacent nodes are experienced by nodes in the network. The said events will establish direct trust relationships in neighborhood nodes. This requires that the reputation of nodes will be taken into deliberation while evaluating trust in other nodes [11].

The trust that is developed depending upon the recommendations given by other nodes is considered by reputation agent. In the same way, its own recommendations will also be discharged to other requesting nodes. The direct trust values can be dispersed by two possible mechanisms: Integrated Reputation Exchange and independent reputation exchange. The existing control or data packets are utilized to spread reputations in Integrated Reputation Exchange. The special packets are used to request and receive trust information in Independent Reputation Exchange[6].

A. Integrated Reputation Exchange

In this scheme, the subsequent data connections or route discovery process are used to spread the trust information. The direct trust values are piggy-backed onto the control or data packets, which acts as a carrier and permits trust dispersal afar of single hop.

The direct trust information of nodes can also be spread by using ROUTE_REP packets shown in Figure 2. The direct trust value can be appended to the ROUTE_REP packet by every node acting as a forwarder in an fragmentary route discovery session, which was send by the former node [5]. The knowledge about trust in the network can be distributed by remaining nodes through ROUTE_REP packets in a direct or indirect manner.

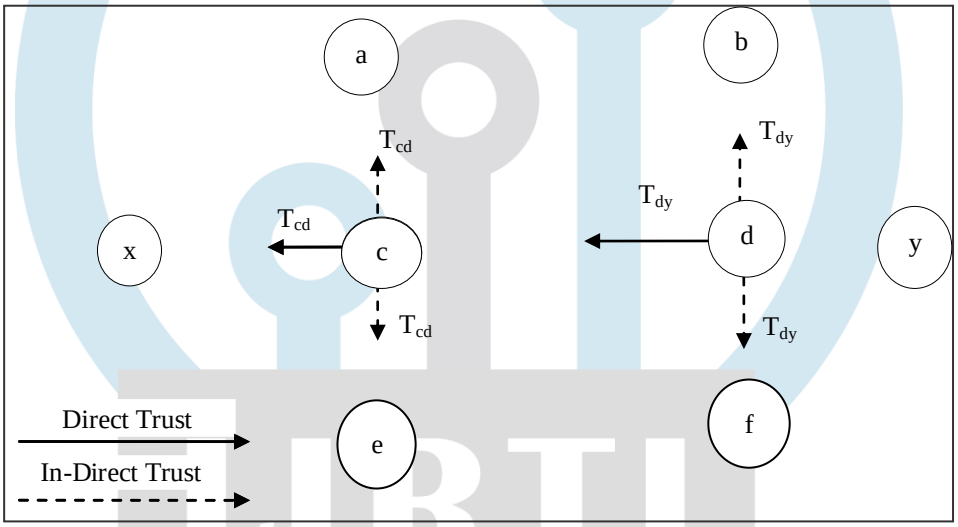

Figure 2: Route-Reply Packets by Trust Propagation

The trust level of node y and d and that of node d to node x will be directly disseminated by ROUTE_REP packet from node y to node x. In addition, the nodes y and d trust levels can be converse to nodes b and f and nodes a ande respectively in an indirectly manner. However, the ROUTE_REP packets need to be initiated for the updating of trust information. The trust information can be spread all over the network due to the flooding nature of the selected carrier by using ROUTE_REP packets.

The real time reputation exchange can be obtained by using data packets as a carrier. This technique avoids the additional packets for reputation exchange and dependent upon the type of carrier selected. These mechanisms can influence the trust dispersal efficiency and throughput of the network.

B. Independent Reputation Exchange

The functionality of the higher layer protocol is exchange of recommendations between the Recommender and Requester that can be periodically employed on requirement.It is proposedto use Hash-Cash [2] tokens with recommendations to control the spread of erroneous requests and replies. The CPU computes Hash-Cash cost function for proof-of-effort token by using a hash function. This token is derived by either interactive or non-interactive situation.

The recommender issues confront to the requester in the interactive setting. After resolvestheconfront, the requester returns the outcome in the token format to the recommender. The token is verified by recommender to validate the proof-of-effort with the help of requester.

The requester calculates a recognized challenge, which depends on available information and returns a token to the recommender in the non-interactive setting. The verification is simple by recommender instead of solving the challenge by requester. The token presented by the requester is backed by a validated proof-of-effort.

The cryptographic hash functions are used to compute the HashCash tokens. The following Table1 shows the format of the HashCash token.

Version	Time	Resource	Trial
1.2	13, 5, 21, 11, 43, 15 (YY, MM, DD, HH, MM, SS)	string	random_start()

Table1: Time Format of the HashCash Token

The type of the hash function engaged is indicated by Version number. The present date and time is specified by Time. The requester and recommender negotiate the challenge string represented by Resource. The Trial is the string that events to perform by the requester.

While generating the token, various combinations of the trial string is used to find a token by requester. This may causes a certain number of most significant bits (MSB) as zero. The amount of work that the requester has to carry out before finding a prejudiced collision is determined by MSBs. The recommender can be verifying the token, which is received from requester by a single hash operation.

In non-interactive setting, the Hash-Cash is used to decrease the number of exchange messages. The Recommendation Request (REC_REQ) packet is sent by requester and the recommender gives the response by a Recommendation Reply (REC_REP) packet, which indicates the reputation of requested node.

The REC_REQ packet contains different identities along with a Hash-Cash token. The different identities and other fields, which are contained in Recommendation exchange Protocol used for recommendations exchange between nodes. The different identities in recommendation exchange protocol are described in Figure 3.

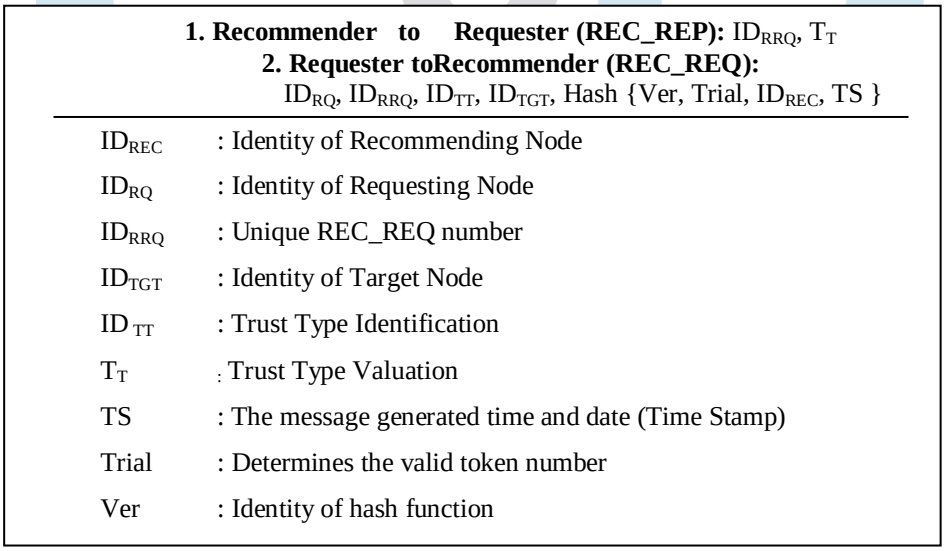

Figure 3: Different Identities in Recommendation Exchange Protocol

The hash function identification and a timestamp (TS) can identify the recommender and a trial number contained by a Hash-Cash token. When the token is hashed, the Trial number is found randomly and causes to achieve a certain number of zeros in the MSBs. The more time will be taken to generate the token, if the MSBs are higher.

When the recommender receives the REC_REQ packet, it verifies the permitted time threshold value just above TS. The loosely synchronized clocks generate the threshold value and can be adjusted depending upon the strongly opposed environment.

The necessary quantity of zeros in the MSB of the hash will be determined by the Hash-Cash token.

The sender has spent a quantity of exertion prior to creating the REC_REQ packet, if and only if the resultant is true. The recommender responses with a REC_REP packet, which contains 2-tuple (IDTGT, IDTT), REC_REQ identification number (IDRRQ) and value of Trust Type (TT). All these values are getting from the situational table and trust table [4].

The reputation received by a node from its adjacent neighbour's logged format is shown in Table 2.

Node	x	y	z	…	…
x	--	$T_{\underline{xy}}$ $T_{\underline{xy}}(1)$ $T_{\underline{xy}}(2)$ … $T_{\underline{xy}}(n)$	$T_{\underline{xz}}$ $T_{\underline{xz}}(1)$ $T_{\underline{xz}}(2)$ … $T_{\underline{xz}}(n)$	…	…
y	$T_{\underline{yx}}$ $T_{\underline{yx}}(1)$ $T_{\underline{yx}}(2)$ … $T_{\underline{yx}}(n)$	...	$T_{\underline{yz}}$ $T_{\underline{yz}}(1)$ $T_{\underline{yz}}(2)$ … $T_{\underline{yz}}(n)$	…	…
z	$T_{\underline{zx}}$ $T_{\underline{zx}}(1)$ $T_{\underline{zx}}(2)$ … $T_{\underline{zx}}(n)$	$T_{\underline{zy}}$ $T_{\underline{zy}}(1)$ $T_{\underline{zy}}(2)$ … $T_{\underline{zy}}(n)$	...	…	…
…	…	…	…	…	…

Table 2: Reputation Table

The present status of the trust of the nodes in the network can be obtained by the continuous receipt of reputations.

The value of direct trust ofnode y, sent by node x, is symbolize as Txy. The value of situational trust of node y, sent by node x in a situation n (trust category n) is represented as Txy(n).

III. Trust Agent

The division of the functions of trust agent is shown in Table 3, with respect to OSI reference model and TCP/IP protocol suite. The three functions of trust agent are derived at appropriate layers of OSI reference model and TCP/IP protocol. Table 3 depicts the same context. In MANETs, the routing protocols basically follow either OSI reference model or TCP/IP protocol suite.

A trust agent derives the direct and situational trust relationships between the nodes in the network at different layers of OSI reference model and TCP/IP protocol suite [10].

OSI Reference Model	TCP/IP Protocol Suite	Division of Tasks
Application Layer	Application Layer	Quantification and Evaluation
Presentation Layer		
Session Layer		
Transport Layer	Transport Layer	Derivation
Network Layer	Internet Layer	
Data Link Layer	Host to Network Layer	
Physical Layer		

Table 3: Division of Tasks by Trust Agent

A. Derivation of Trust

In the passive mode, the useful information such as forwarded data packets, received data packets, forwarded control packets, received control packets, frames received and streams established can be collected by adjacent nodes and then examines the traffic. The special control packets are not necessary to carry out the derivation network of the trust. In the protocol stack, the above said events are analyzed at different layers.

These measures are split into one or more situational trust categories by the acquired information. The situational trust values are provided by trust categories.

B. Quantification of Trust

The quantification of trust with discrete values is not sufficient to represent the trust. In the projected model, the quantification of the trust is derived in a continuous mode.

The trust is represented in a binary form in secure routing protocols by either the absence or presence of security.

In a distributed trust mode [1], the quantification of trust is done in a discrete mode with six intervals from complete trust to distrust.

Similarly, he also proposed in Pretty Good Privacy model, the trust is quantified with four intervals from trust to distrust.

Discrete values are not appropriate for application to MANETs, but used to categorize the trust. The trust relationships are consistently altering due to the dynamic topology, and hence the trust in MANETs is dynamic.

In the proposed trust model, the trust values ranges from 0 to 1 are considered. Here, 0 means distrust and 1 indicates complete trust.

IV. Computation of Trust

The weights such as beacon messages, packet precision, gratuitous route replies, unreachable messages to destination, passive acknowledgements and savaging are assigned to the formerly quantified and monitored events during trust computation. The computed weights are dynamically allocated to all the nodes due to their situation and own criterion. The values of above said weights in AODV, DSR and TORA protocols are specified in the Table 4.

Situational Trust Category	Weights	Protocol		
		AODV	DSR	TORA
Beacon / HELLO Messages	W (H_M)	0.05	--	0.11
Black Lists	W (B_L)	--	--	--
Packet Precision	W (P_P)	0.6675	0.6675	0.6675
Gratuitous Route Replies	W (G_R)	0.04	0.04	--
Unreachable Messages to Destination	W (U_D)	0.02	--	--
Passive Acknowledgements	W (P_A)	0.2225	0.2225	0.2225
Authentication Objects	W (A_O)	--	--	--
Salvaging	W (S_G)	--	0.07	--

Table 4: Optimal Weights at different Situations

The low values of weights indicate unimportant and high values of weights indicate most important. A node's direct trust value can be calculated by the combination of situational trust categories. The following equation gives the node y's direct trust valueby node xand represented as Txy.

$$T_{xy} = \sum_{i=1}^{n} \left(W_{xy}(i) * T_{xy}(i) \right)$$

Where Wxy(i) is the i^{th} trust category weight of y node to xnode.Txy(i) is the i^{th}trust category situational trust value of x node in the node y. Here, n is the whole number of trust categories that are applied to the trust model which depend upon the scenario and protocol[8]. The direct trust rating in relation to other nodes in the network is maintained by every node in the network. This is represented in Figure 4.

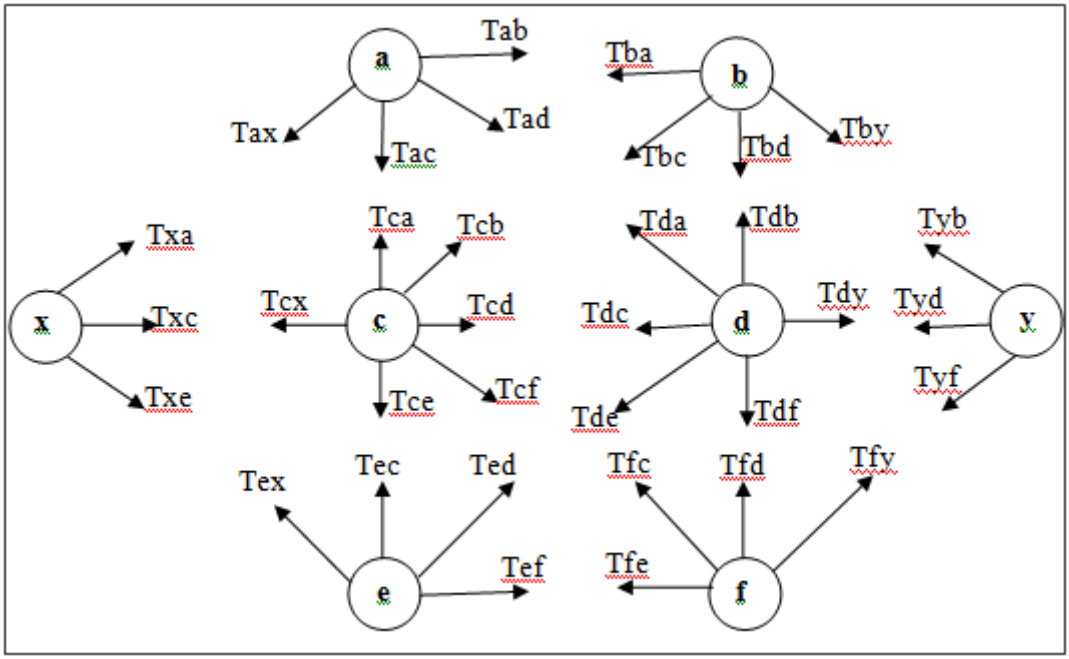

Figure 4: Relationships of Direct Trust

The values of direct and situational trust are dynamically updated and maintained to represent the present trust significance of nodes. The direct and situational trust values are from the point of view of node y is shown in Table 5.

Node	Situational Trust in Category					Direct Trust
	1	2	…	…	*n*	
b	$T_{yb}(1)$	$T_{yb}(2)$	…	…	$T_{yb}(n)$	T_{yb}
d	$T_{yd}(1)$	$T_{yd}(2)$	…	…	$T_{yd}(n)$	T_{yd}
f	$T_{yf}(1)$	$T_{yf}(2)$	…	…	$T_{yf}(n)$	T_{yf}

Table 5: Direct and Situational Trust Table

V. TRUST MIXER

The trust mixer obtains the values of trust from the reputation and trust agents. The whole trust value of an intention node can be computed by probabilistic computing method. The probabilistic computing method is adopted and modified by Beth. T. [Beth. T. et al., 1994].

In general, the trust computing methods [3, 12] are used for trust values combination. This process with an example is described as shown in Figure 5.

In between x node and z node the direct trust is represented by Txz and the received trust which is recommended from z node between z node and ynode is represented by Tzy, then the Txzyis the trust derived between x node and ynodeusing node z is shown below:

$$T_{xzy} = T_{xz} \otimes T_{zy} = 1 - (1 - T_{xz})$$

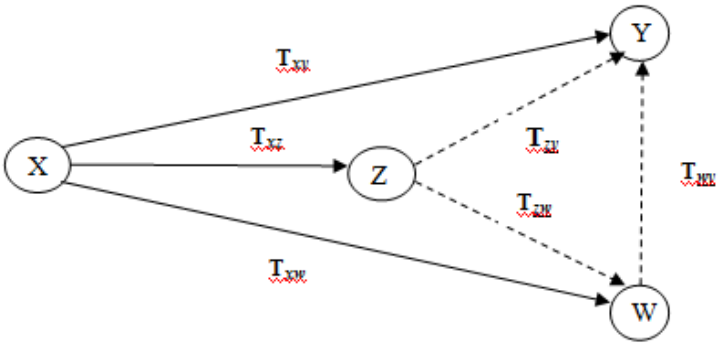

Figure 5: Derivation of Trust Relationships

Similarly, the derived trust between node x and node y through node w, is represented by Txwy is formulated as follows:

$$T_{xwy} = T_{xw} \Theta T_{\underline{wy}} = 1- (1 - T_{xw}))$$

is the trust derived amid node z and node y through node w is unacceptable knowledge of any direct trust and thus described as follows:

$$T_{zwy} = T_{\underline{zw}} * T_{\underline{wy}}$$

The summative trust between xnode and y nodeis represented as T(y) is computed from the direct and derived trust values as follows:

$$T(y) = 1- (1- T_{xy}) * (1- T_{xzy}) * (1- T_{xwy})$$

Node Name	Direct Trust	Recommended Trust	Aggregate Trust
a		$T_{yba} = 1- (1- T_{yb})^{T_{\underline{ba}}}$ $T_{yda} = 1- (1- T_{yd})^{T_{\underline{da}}}$	$T(a) = 1- (1-T_{yba}).(1- T_{yda})$
b	T_{yb}	$T_{ydb} = 1- (1- T_{yd})^{T_{\underline{db}}}$	$T(b) = 1- (1-T_{yb}).(1- T_{ydb})$
c		$T_{ybc} = 1- (1- T_{yb})^{T_{\underline{bc}}}$ $T_{ydc} = 1- (1- T_{yd})^{T_{\underline{da}}}$ $T_{yfc} = 1- (1- T_{yf})^{T_{\underline{fc}}}$	$T(c) = 1- (1-T_{ybc}).(1- T_{ydc}).(1-T_{yfc})$
d	T_{yd}	$T_{ybd} = 1- (1- T_{yb})^{T_{\underline{bd}}}$ $T_{yfd} = 1- (1- T_{yf})^{T_{\underline{fd}}}$	$T(d) = 1- (1-T_{yd}).(1- T_{ybd}).(1-T_{yfd})$
e		$T_{yde} = 1- (1- T_{yd})^{T_{\underline{de}}}$ $T_{yfe} = 1- (1- T_{yf})^{T_{\underline{fe}}}$	$T(e) = 1- (1-T_{yde}).(1- T_{yfe})$
f	T_{yf}	$T_{ydf} = 1- (1- T_{yd})^{T_{\underline{df}}}$	$T(f) = 1- (1-T_{yf}).(1- T_{ydf})$

Table 6: Direct, Recommended Trust and Aggregate Trust Table

The trust mixer maintains and dynamically updates the derived and aggregate trust values, whenever the occurrence of change either in the reputation table or direct and situational trust table[7]. The above Table 6 shows the direct trust, recommended trust and aggregate trust for ynode of Figure 5.

VI. SUMMARY

In this chapter, a trust model is presented without requirement of third party trust.The established trust by trust model is maintained trust in the MANET. The trust is established in MANET without any superfluous assumptions, requirements and cryptographic mechanisms are proposed in the trust model.

Depending upon preceding and contemporary actions by all adjacent neighbors, the trust agent in the trust model is used to derive, quantify and compute direct trust levels. The trust agent verifies the sincerity in the execution of the routing protocol and integrity of forwarded traffic. The trust agent is also responsible for packet forwarding events.

The nodes can make use of an independent or integrated reputation exchange mechanism to share reputations, when the nodes are not in vicinity. The underlying routing protocol is used as a carrier to propagate direct trust values, when the integrated reputation mechanism is considered. In case of independent reputation exchange mechanism, a separate higher level protocol is used as the carrier.

The single aggregate trust value is obtained by combining these direct trust values and reputations. The aggregate trust value is used to differentiate between trustworthy and untrustworthy nodes.

This trust model can be applied to improve the routing performance in a network under attack conditions in reactive routing protocols like AODV, DSR and TORA.

REFERENCES

[1] Rahman. A. A. and Hailes. S. : 1997, "Using Recommendations for managing Trust in distributed systems", Proceedings IEEE Malaysia International Conference on Communication (MICC '97), Kaulalampur, Malaysia,

[2] Beth. T., Borcherding. M. and Klein. B. : 1994, "Valuation of Trust in Open Networks", Proceedings of the Third European Symposium on Research in Computer Security (ESORICS), Springer- Verlag, Pp. 3-18.

[3] Deepa. P., Shalini. A. and Jukkulin Joshi. J. : 2011, "Trust Management for Mobile Ad hoc Networks using Recommendation Exchange Protocol", International Journal on Computer trends and Technology, May-June Issue, Pp. 122-128.

[4] Baras. J. S. and Jiang. T. : 2004, "Dynamic and Distributed Trust for Mobile Ad hoc Networking", Prepared through collaborative participation in the communications and networks Consortium, Army Research Laboratory, Maryland, Orland, USA.

[5] Liu. J. and Issarny. V. : 2004, "Enhanced Reputation Mechanism for mobile Ad hoc Networks", Proceedings 2nd International Conference of trust Management (iTrust 2004), Oxford, UK, Pp. 48-62.K.Elissa, "Titleofpaperifknown," unpublished.

[6] Davis. C. R. : 2004, "A localized trust management scheme for Ad hoc Networks", Proceedings 3rd International Conference on Networking (ICN '04), Pp. 54-58

[7] Liu. Z., Joy. A. W. and Thompson. R. A. : 2004, "A Dynamic Trust Model for Mobile Ad hoc Networks", Proceedings 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, Pp. 80-85.

[8] Rahman. M. G. and Mohammed Ghulam : 2011, "A Trust based MANET Routing Protocol", 17th Asia-Pacific Conference on Communications. Pp. 542-547.

[9] Li. J., Li. R., and Kato. J. : 2008, "Future Trust management framework for mobile Ad hoc networks: Security in mobile Ad hoc networks", IEEE Communications Magazine, Vol. 46, No. 4, Pp. 108-114.

[10] Ahmed M. Abd El-Haleem and Ihab A. Ali : 2011, "TRIDNT: The Trust based Routing Protocol with Controlled degree of node Selfishness for MANET", International Journal of Network Security & its Applications, Vol. 3, No. 3, Pp. 189-204.

[11] Edwin Prem Kumar. G., Titus. I. And Sony. I. Thekkekara : 2012, "A Comprehensive Overview on Application of Trust and Reputation in Wireless Sensor Network", 38th International Conference on Modeling Optimisation and Computing, ScienceDirect, Pp. 2903-2912.

[12] RenuDalal, Manju Khari and Yudhvir Singh : 2012, "Different ways to achieve Trust in MANET", International Journal on Adhoc Networking Systems, Vol. 2, No. 2, Pp. 53-64.