IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Identify And Remove Time And Location Dependent Attack Using Trust Concept for MANETs

Namrata Kumari[1*], Chetan Agrawal[2], Pooja Meena [3]

[1,2,3]Dept. of CSE, Radharaman Institute of Technology & science, Bhopal, India

[*]*Corresponding Author: namo2094@gmail.com, Tel.: +91-8109816382*

Available online at: www.ijcseonline.org

Accepted: 18/Oct/2018, Published: 31/Oct/2018

***Abstract*—** One of the sort of ad-hoc network is Mobile ad hoc networks (MANETs). MANETs are making them arrange and owned formulated network and there is no concentrated base station. In routing forwarding the data packet between nodes is core issue due to badly behaving or untrustworthy nodes present in the network. Recommendation trust model is a framework to find out the untrustworthy nodes and provide routes for packets to destination. A trust demonstrate takes recommendation by nodes transforms into an issue in light of the nearness of deceptive proposition like as ballot-stuffing, bad-mouthing and collusion. Untrustworthy nodes in the existing trust models lead to attacks by using recommendation which is investigated in this paper. Time and Location Dependent Attack Detection (TLDAD) Approach has been proposed in this paper to successfully sift through attacks identified as dishonest recommendation. The fundamental commitment of this work is to identify and remove time and location dependent attack related to recommendation Trust Model in MANETs. The model is tested under a couple of mobile and isolated topologies within which nodes find some changes in neighborhood provoking regular course changes. This paper focuses on a secure communication path across the nodes in the network. The experimental examination shows activeness and accuracy of the proposed method in a dynamic MANET condition.

***Keywords*—** Mobile ad hoc networks, Dishonest recommendation, Trust management, Recommendation Trust Model , Time and Location Dependent Attack

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a classification of the wireless ad hoc network. A network in which gathering of remote portable hubs that are fit for speak with each different hubs with no settled foundation is Mobile Ad hoc Network [1]. MANET is additionally fit for engendering self-configuring and self-maintaining architecture while not the desideratum of any concentrated infrastructure, typically possible in vital applications like military conflict, emergency accommodations [2], [3]. These characteristics make MANET yare to be utilized in emergency circumstances where such centralized infrastructure is unavailable. One of the real advantages of wireless networks is its faculty to sanction data communication between different gatherings and still maintain their mobility. Because of unique property and appeal use, MANETs are powerlessly defenseless to attacks caused by misbehaving nodes [4]. In MANET trust can be characterized as a bore of confidence as indicated by the actions of nodes [5]. Trust is the conclusion given by a single node (admitted as evaluating node) concerning other node (admitted as evaluated node), predicated by node's past deportment and suggestions by different node (admitted as recommending node) in the network[5]. In the absence of previous communication, a specific node probably won't be especially assessed to make an evaluation of reliability of other node. In that situation, the evaluating node considers suggestions from the evaluated node's neighbors with whom it has a previous filled with interaction. Sifting through ambiguous suggesting nodes turns into a quiet trouble while prescribing nodes conspire with each other to achieve a malicious objective [6].

A few nodes in the network not proceed from the path deciding protocols rules and creating adverse environment in the Ad-Hoc Network. In this type of situations, we worked on recommendation trust model. A trust show use suggestions by nodes turns into an issue in light of the presence of deceptive approach like ballot-stuffing, bad-

mouthing and collusion. Increasing suggestions in the present trust models lead to attacks occurred by bad nodes.

The design goals of this work are creating a trust domain for MANET. We are using scheme for the detection of Time and Location related attack and remove and increase network throughput and decreases the packet loss. Our results display that the tender algorithm decreases the packet loss up to 2% and increases the throughput up to 3%.

Remaining paper is systemized as given. We are showing attacks focused during recommendation management in Segment II. Details of trust management are presented in Segment III. In Segment IV our trust model is explained. We expose the related works in Segment V. In segment VI, proposed algorithm is explained. Segment VII shows our simulation and results. In Segment VIII we present our conclusions and future work.

II. ATTACKS FOCUSED DURING RECOMMENDATION MANAGEMENT

The following attacks are focused during recommendation [7], [8], [9].The attack behaviors are summarized as below:

A. Bad mouthing attack (BMA). In this attack, malicious nodes can give fraudulent recommendations to outline up good gatherings and/or increase trust rate of malicious nodes. This attack is mentioned as BMA. The blocking of original routes by such kind of fraudulent behavior in the network by misguiding the trust management.
B. Ballot stuffing attack (BSA). Generation of positive reviews which are fake for some fraudulent nodes by some nodes tends to attack in network. The motive of fraudulent nodes is to misguide the trust concept and trigger glitch the faith of analyzed node.
C. Selective misbehavior attack (SMA). This attack misguide some reliable nodes by providing false rate for them, meanwhile it behaves usual to other nodes.
D. Intelligent behavior attack (IBA). This attack accordingly gives commendation with fluctuating rates suitably to the trust threshold. This type of attacks tends to failure of trust structure by effectively giving response to trust threshold and perform accordingly.
E. Time-dependent attack (TDA). Performing nodes behave differently according to time is known as TDA and this can mischief by giving unusual grading at different times.
F. Location-dependent attack (LDA). Mobility characteristics of MANETs leads to LDA, where nodes show its characteristics based on location. This attack occurs due to intuitive characteristics of trust where performance at one location is not overripe reliability of nodes at some other location.

III. TRUST MANAGEMENT

The trust of categorical node depends on subjective judgments by peer/agent node on reliability and obtaining data from and (or) traversing by the node provided situation and time. The primary features of confide in MANET have subjective, dynamic, context dependency and asymmetry. Trust can be evaluated in perpetual value in between [0,1]. Two kind of trust one is direct and indirect. Direct trust depends on identity of nodes. This can be acquired by digital signature, encryption mechanism and authentication technique. Indirect trust depends on actions of nodes and is utilized to differentiate between bad and good node. Comportment trust can be demonstrated as in and directly. A direct trust is examination which automatically built by the node alone. Indirect trust is quantified utilizing advice from different nodes, and suggests trust from third party in MANETs. For every node, Trust management is to quantify the adjoin nodes demeanor, and allocates a trust rate depending on the behavioral assessment result [7]. Trust frame are carried for trust management. These trust model are categorized as dispersed and centralized structure. Trust rate are preserved in authenticated third party server or centralized server in centralized models, since this model is not felicitous because of dynamic transmuting configuration as MANET. Every node allocates trust rate to its adjacent nodes to communicate with different node in decentralized structure .Nodes within the communication range are taken to be the adjoin nodes. In starting, a node is not kenned of the considerable number of nodes in the communication area. To demonstrate confide in MANET a node must vigilant all the adjoin nodes with in network.

Trust management ameliorates the privacy and defense of MANETs and withal enhances the communication quality among contrivances [7].

IV. RECOMMENDATION TRUST MODEL

The ballot-stuffing, bad-mouthing and collusion are separated as dishonest recommendation for MANETs by

recommendation trust model. The node which is a recommending node is accepted by some aspects to find out its honesty: Number of correspondence between nodes, Affinity of data with the evaluated node for providing the solution of the shortage of information, accessible to the evaluating node. Recommendations are aggregated over some stretch of duration to guarantee the uniformity of recommendations provided by a suggested node in consideration to the evaluated node. Clustering process is used to separating the recommendations between certain period allotment in light of:

a) Number of correspondence
b) Affinity of data with the evaluated node
c) accessibility between the nodes.

Many nodes are chosen in the demonstrating approach to find the execution of the separating algorithm with many mobile topologies and neighborhoods.

Three segments of model situated to assess trust:

(a) Trust Computation segment which access direct and indirect trust data.
(b) Recommendation Manager segment that appeals and collects suggestions for a node from the record of suggested nodes.
(c) Cluster Manager Segment that remove fraudulent suggestions from the list and send out a record of honest suggestion to the manager segment.

V. EXISTING WORK

Authors in [10] offered RFS Trust, a trust model in view of fuzzy recommendation resemblance, that is exhibited to measure and assess the dependability of nodes. They utilize similarity hypothesis to assess the suggested connections with in nodes. Higher the value of resemblance between the evaluating and the suggested node, the more predictable is the computation within two nodes. In this structure, just a single kind of circumstance is examined that is selfish node attack and the execution of the structure isn't tried against different attacks identified with endorsement.

In a venture to improve the integrity of utilizing suggestions, Li et al in [6] takes a confidence term in their assessment by consolidating two things: confidence and trust combined to form trustworthiness. They use the trustworthiness data to give mass on recommendations in which more weightage is given to the suggested node with higher trustworthiness. Collusion attack gives bad suggestions is not taken in this work, and this may origin mistaken assessment of the accepted suggestions.

Hermes [11] is a recommendation based trust structure which introduces a concept that is acceptability threshold. The thought of holding ability is utilized in the calculation of recommendation to verify that sufficient examination of the behaviour of engaged node has been acquired. Yet the process of intelligibility is a trade-off between getting more close trust worthiness value and time needed to acquire it.

A recommendation exchange protocol (REP) is proposed by Pedro B. et al. [12] to enable nodes to send and receive recommendations from neighbouring nodes. It presents the idea of relationship maturity in view of to what extent nodes have known one another. Recommendations sent by long term associates are weighed higher than that from short term associates. The maturity of relationship is assessed based on a single factor by considering just the duration of relationship.

Yu et al. in [13] propose a clustering procedure for separating reliable suggestion from unreliable ones. They focuses on the predominance law by choosing the cluster with the maximum number of suggestion as reliable one. Bad mouthing and ballot stuffing attack demonstrated by this system. On the other hand, predominance law could not be in favour because of conspiring node and not deliver a correct opinion about other nodes.

VI. ALGORITHM FOR PROPOSED MODEL

In our implemented method, at first network configured and the sender node is established. Afterward, the suggested algorithm assembles the data from the adjoin log statements to identify the accomplishment or breakdown numbers of packets counter inside the nodes. The trust value is evaluated depend on the sequence ID of packet, which is identical in contrast of log statements of the nodes. Primarily, DSR is a reactive protocol of routing which locates the paths at the time of requirement, by employing the destination sequence numbers to acquire the freshest path. Because of this, DSR establishes the latest path to the receiver node.

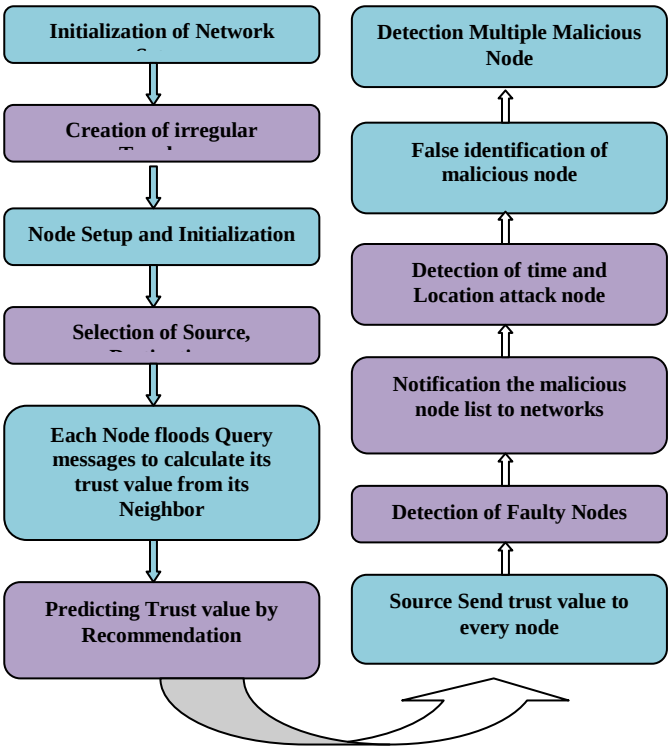

Figure1. Flowchart of Proposed Algorithm

Time and Location Dependent Attack Detection Approach (TLDAD):

1. Setup the complete environment and configurations.
2. Initialize the node population xí=(í = 1,2…n) and more initialize every one of the nodes , setup the position for every node for movement.
3. Define neighbour node and its frequency *f*í at xí
4. Initialize the Trust the(trust) Tí
5. While (t < Maximum no. of iterations)
6. Produce new solutions through adjusting frequency, traffic, by modifying values, and updating Time and locations/solutions

$$Fi = F_{min} + (F_{max} - F_{min})\beta,$$
$$Vi^{t+1} = Vi^{t} + (Xi^{t} – X^*)Fi ,$$
$$Xi^{t+1} = Xi^{t} + Vi^{t} ,$$ - Bat Equation Using Bat.

7. Execute Bat algorithm on outcome solution

TLDAD = (Ti); finding similar pattern.
Check Trust of neighbour node.
Accept the new solutions
Repeat 1-7 until simulation time end;

VII. SIMULATION AND RESULTS

7.1 Simulation Parameters

NS2 is an open-source discontinuous simulator which is mainly used for simulation. In computer networking, NS2 plays a vital role to enhance research. It includes diverse modules [14]. NS2 includes some network components like application and transport layer protocols, packet and node routing for testing many modules.DSR routing protocols are expanded by NS2 which reinforce architecture of MANETs.

Table 1. Network Configuration Parameters

Parameter	Value
Simulation Area	700m * 700m
Simulation Time	500 seconds
Number of Nodes	50
Radio Range	250 m
Node Speed	10 m/s
Routing Protocol	DSR
MAC	802.11
Source-destination pairs	15
Transmitting capacity	2 Kbps
Application	CBR
Packet size	512 B
Visualization Tool	Nam

Within the area of 700*700 square meters, 50 dynamic mobile nodes are added to form a network. Nodes are frequently chosen as faulty node in the form of location and time dependent attack. Here 15 pairs are selected as source and destination for communication and with a Constant bit rate (CBR), every source is forwarding 2 packets per second and node speed is 10m/s.

7.2 Performance Metrics

As per the following stream, the simulation goes on. In the presence of dishonest recommending nodes, two parameters show the entire network performance: Network throughput and Packet Loss. To see the impact of location and time dependent attacks, trust value related to a node is assessed versus time and distance parameters for know how an attacker alters the node's trust value.

7.2.1 Throughput Vs Dishonest Recommendation

The percentage of throughput shown in Fig-2, from below graph we are able to see two completely different graph lines that are Existent and proposed work. Inside the graph x-axis and y-axis show Dishonest Recommendation and throughput severally. The y-axis, with the presence of dishonest

recommendation nodes varying from 0 to 80 percent of the total population of nodes. It is ascertained that the network throughput of no defence falls from nearly 80 percent when the dishonest recommending nodes are absent to nearly 40 percent when population of the dishonest ones increases to 35 percent. Slight decrease and after that increase is seen in throughput for the network of existent when the percentage of dishonest recommendation nodes increases from 20 to 25 percent. From Fig-2 we can see that the proposed mechanism can give somewhat high value of throughput when dishonest recommending nodes are absent as compared with no defence and existent. This is additionally able to keep the value of throughput at nearly 80 percent even in case of high population of the dishonest nodes. Hence from above we can state that we are improving throughput utilizing proposed approach of the network.

Table 2. Throughput Vs Dishonest Recommendation

Dishonest Recommendation	No Defence	Existent	Proposed
10%	0.80	0.81	0.84
15%	0.69	0.79	0.83
20%	0.63	0.79	0.81
25%	0.55	0.78	0.80
30%	0.51	0.77	0.79
35%	0.40	0.77	0.78

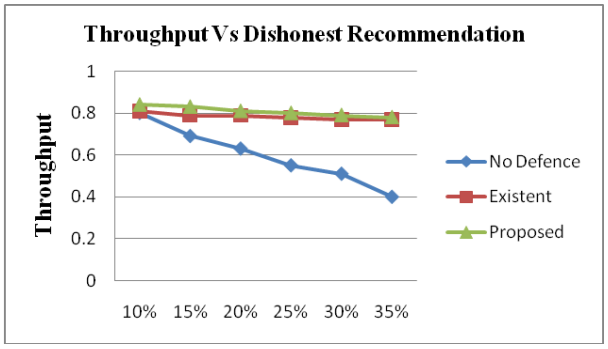

Figure 2. Throughput Vs Dishonest Recommendation

7.2.2 Packet Loss Vs Dishonest Recommendation

The percentage of packet loss represented in Fig-3, from below graph we are able to see three different graph lines that are Existent and proposed work. In the graphs x-axis and y-axis show Dishonest Recommendation and packet loss respectively. From the graph we can observe that the percentage of packet loss increases with increasing the percentage of dishonest nodes from 15 to 35 percent in case of no defence. However, the percentage of packet loss decreases in case of existent when the percentage of dishonest nodes is 10 percent and marginally increases from 15 to 35 percent however compare to no defence the packet loss is less in percentage. Now in case of proposed mechanism, the percentage of packet loss decreases as compared with no defence and existent. Subsequently it tends to be seen from above that the packet loss is reduced using proposed approach of the network.

Table 3. Packet Loss Vs Dishonest Recommendation

Dishonest Recommendation	No Defence	Existent	Proposed
10%	0.20	0.19	0.18
15%	0.31	0.20	0.19
20%	0.39	0.21	0.20
25%	0.43	0.22	0.20
30%	0.48	0.22	0.21
35%	0.60	0.23	0.22

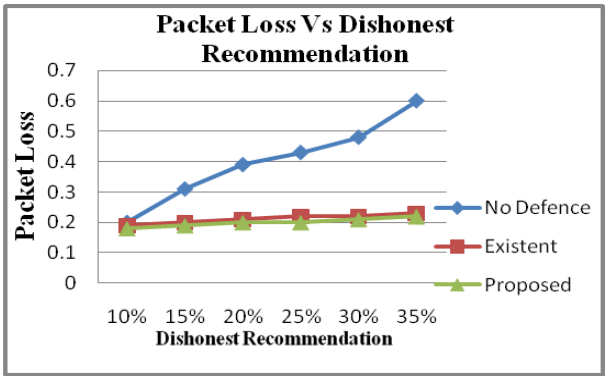

Figure 3. Packet Loss Vs Dishonest Recommendation

7.2.3 Node Trust value Analysis on Time Dependent Attack

Execution of our approach is estimated based on Node Trust value Vs. Time. We are looking at between Expected trust values and proposed trust values. Fig-4 exhibits the average of the trust values held by other nodes in the network. The x-axis shows the range of the simulation time for a node (node 8 in this case) from 0 to 250 sec. The y-axis shows the average of trust value for a node (node 8 in this case). A comparison has been made between three different parameters as follows. To start with, the trust value when there are no dishonest nodes, called expected value. Second, the trust value when the dishonest nodes are available and the defence technique is not

working, no defence. Third, the trust value when dishonest nodes are available and defence scheme is working, proposed. It tends to be seen that as for simulation time the average trust value of node 8 changes in case of no defence and proposed with respect to expected. The trust values are less than expected and proposed in case of no defene. Expected and proposed trust values are same. It is showing the time dependent attack property of node 8 that is changing its behavior by time which is represented by changing its trust value in network.

Table 4. Time Vs Node Trust Value

Time (Second)	No Defence	Expected	Proposed
0	0.65	0.98	0.98
50	0.79	0.97	0.97
100	0.85	0.97	0.97
150	0.60	0.96	0.96
200	0.75	0.95	0.95
250	0.55	0.93	0.93

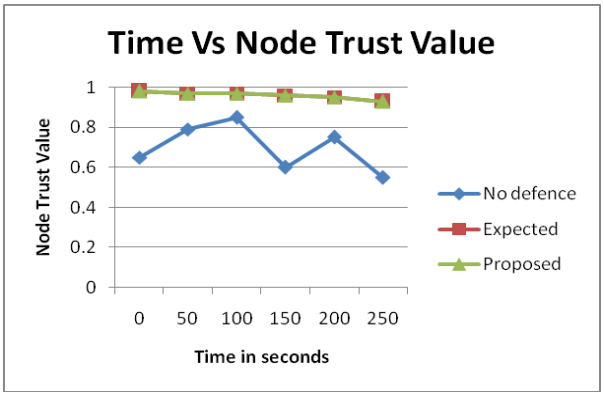

Figure 4. Time Vs Node 8th Trust Value in Time Dependent Attack

7.2.4 Node Trust value Analysis on Location Dependent Attack

The effect on trust value is shown is fig-5. In the x-axis is the distance of node (node 23 in this case) which is used to shows the location of the node in the network area of 700m*700m varies between 0 to 700 meter which is calculated by taking speed of node 10m/s and a constant time interval 10s and y-axis represents the values for the trust compare against the same three parameter i.e. expected value, no defence, proposed case. First, the trust value when there are no dishonest nodes, called expected value. Second, the trust value when the dishonest nodes are available and the defence technique is not working, no defence. Third, the trust value when dishonest nodes are available and defence scheme is working, proposed. It can be seen that with respect to distance the average trust value of node 23 changes in case of no defence and proposed with respect to expected. The trust values in case of no defence are less than expected and proposed for node 23. In proposed scheme the trust value is equal to expected but more than the no defence case and shows the property of the location dependent attack. It is showing the location dependent attack property of node 23 that is changing its behavior based on location that is shown by changing its trust value in the network.

Table 5. Distance Vs Node Trust Value in Location Attack

Distance(meter)	No Defence	Expected	Proposed
0	0.90	0.98	0.98
100	0.75	0.97	0.97
200	0.79	0.97	0.97
300	0.71	0.96	0.96
400	0.81	0.95	0.95
500	0.85	0.94	0.94
600	0.69	0.93	0.93
700	0.78	0.91	0.91

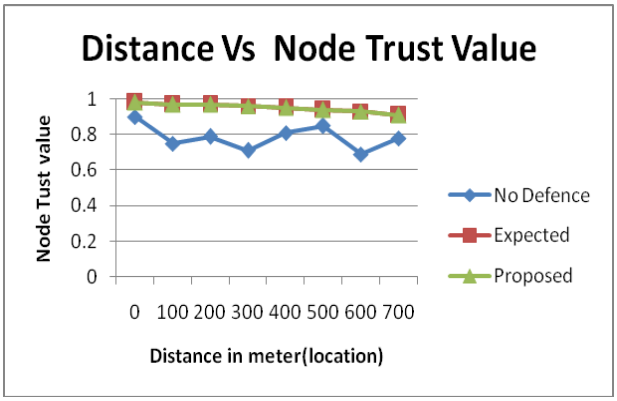

Figure 5. A node 23's trust value evaluation with its different Distance(position in simulation area)

VIII. CONCLUSION

In MANETs, end to end delivery of packet ratio is decreased due to a misbehaved node. For incrementing packet distribution ratio here is the requisite for dynamically detecting the misconduct nodes depending on trust rate. The

misbehaving nodes cause Location and Time dependent attacks that are find out by a trust model which accepts recommendation from nodes is talked regarding during this paper. Since dishonest nodes decrease the working of the network therefore the proposed algorithm TLDAD is used to find out the dishonest nodes that lead to the location and time dependent attack. The proposed TLDAD algorithm is used to enhance cooperation among the nodes depending on efficient trust computation. In terms of throughput and packet loss, the proposed system is examine through considerable imitation against both location and time dependent attacks, and also differentiated with different approach. In extension of my current work, we plan to carry out the model to improving the security in MANETs by using some prevention techniques for misbehaving nodes. We can also apply and evaluate our model in lager-sized MANETs to evaluate its performance in future.

REFERENCES

[1] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, Oct. 200

[2] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: Imperatives and challenges," Ad Hoc Netw., vol. 1, no. 1, pp. 13–64, 2003.

[3] G. Sabeena Gnanaselvi, T.V.Ananthan, "An Analysis of Applications, Challenges and Security Attacks in MANET" , International Journal of Computer Sciences and Engineering, Vol.6 , pp. 941-947, 2018.

[4] P. Gupta, P. Bansal, "Different Attacks and their Defense Line in Mobile Ad hoc Networks" , International Journal of Computer Sciences and Engineering, Vol.6 , pp.176-190, 2018.

[5] Z. Yan, P. Zhang, and T. Virtanen, "Trust evaluation based security solution in ad hoc networks," in Proc. 7th Nordic Workshop Secure IT Syst., 2003, no. 14, pp. 1–10.

[6] R. Li, J. Li, P. Liu, and J. Kato, "A novel hybrid trust management framework for MANETs," in Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Workshops, 2009, pp.251–256.

[7] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput.Appl., vol. 35, no. 3pp, 867–880, 2012.

[8] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surveys, vol. 42, no. 1, p. 1, 2009.

[9] W. Li, J. Parker, and A. Joshi, "Security through collaboration and trust in MANETs," Mobile Netw. Appl., vol. 17, no. 3, pp. 342–352, 2012.

[10] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," Comput. Netw., vol. 53, no. 14, pp. 2396–2407, 2009.

[11] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks," Ad Hoc Netw., vol. 7, no. 6,pp. 1156–1168, 2009.

[12] P.B.Velloso, R.P.Laufer, D.de O Cunha, O.C.M.Duarte, and G.Pujolle, ''Trust management in mobile ad hoc networks using a scalable maturity-based model,''Network and Service Management, IEEE Trans-actions on, 7, (3), pp. 172-185, 2010.

[13] H.Yu, S.Liu, A.C.Kot, C.Miao, and C.Leung, ''Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks'', Communication Technology (ICCT), 2011 IEEE 13th In-ternational Conference on, pp. 1-6, 2011.

[14] T.Issariyakul and E.Hossain,''Introduction to network simulator NS2,''Springer, 2011.

Authors Profile

Miss Namrata Kumari currently pursuing M.Tech from Radharaman Institute of Technology And Science, Bhopal and Studied B.E. CSE at ANNAMALAI UNIVERSITY Chennai.

Chetan Agrawal studied M.E: CSE at TRUBA Institute of Engineering & Information Technology, Bhopal and Studied B.E. CSE at BANSAL Institute of Science & Technology, Bhopal. He is Asst. Prof. in CSE Department at Radharaman Institute of Technology & Science., Bhopal, M.P. India. His area of interest is Social network Analysis, Network Security, Cyber Security, Wireless Network and Data mining.

Pooja Meena studied M.Tech: CSE at Lakshmi Narain College of Technology, Bhopal .He is Asst. Prof. in CSE Department at Radharaman Institute of Technology & Science., Bhopal, M.P. India.

