Enhanced Trust Based Architecture in MANET using AODV Protocol to Eliminate Packet Dropping Attacks

R. Sathish Kumar [#1], A. Aktharunissa[#2], S. Koperundevi[#3] S. Suganthi[#4]
Assistant Professor, Department of Computer Science and Engineering[#1]
B. Tech, Department of Computer Science and Engineering[#2,3,4]
Manakula Vinayagar Institute of Technology, Pondicherry.

Abstract- *MANET is a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. Secure routing is the milestone in mobile Adhoc networks. MANET is vulnerable to attacks from malicious nodes. The proposed trust scheme using AODV protocol calculates the trust between the nodes in MANET to detect and eliminate the malicious nodes from the transmission path. This technique calculates the trust value of all the nodes. It compares the trust values to detect and eliminate the malicious node from the transmission path. If the trust value is less than a trust threshold, the intermediate node is marked as malicious and rejected from the path. The packets are transmitted only through the nodes with high trust value. We experiment this by NS2 with better accuracy.*

Keywords- *Mobile Ad hoc Networks (MANETs), Ad-hoc On-demand Distance Vector (AODV), trust value, malicious node, PDP, Homomorphic linear authenticator (HLA), Proofs of storage (PoS)*

I. INTRODUCTION

A. Manet

The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Mobile nodes that are within each other's radio range can communicate directly, while distant mobile nodes rely on their neighboring MNs to forward packets. Each mobile nodes acts as either a host or a router[8]. A malicious node that is part of the route can exploit itsknowledge of the network protocol and the communicationcontext to launch an insider attack [1].Otherwise, a stand for "Mobile Ad Hoc Network" A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Ficonnection, or another medium, such as a cellular or satellite transmission.

B. Manet vulnerabilities

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network.

Security is an essential service for wireless network communications. However, the characteristics of MANETS pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and nonrepudiation[3].

a) Lack of centralized management

MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

b) Resource availability

Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

c) Scalability

Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

d) Cooperativeness

Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result, a malicious

attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

II. RELATED WORK

In existing system, authors develop an accurate algorithm for detecting selective packet drops made by insider attackers. Existing algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap—a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. The basic idea behind existing method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses). Therefore, by detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop.Our construction also provides the following new features. First, privacy-preserving: the public auditor should not be able to decern the content of a packet delivered on the route through the auditing information submitted by individual hops, no matter how many independent reports of the auditing information are submitted to the auditor[1].The public-auditing problem is constructed based on the homomorphic linear authenticator (HLA) cryptographic primitive [2], [3], which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients.Existing algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets.

III. LITERATURE SURVEY

A. *Provable data possession at untrusted stores*

We introduce a model for *provable data possession* (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote datachecking supports largedata sets in widely-distributed storage system.We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead atthe server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.

B. *Proofs of storage from homomorphic identification protocols*

Proofs of storage (PoS) are interactive protocols allowing a client to verify that a server faithfully stores a file. Previous work has shown that proofs of storage can be constructed from any homomorphiclinear authenticator (HLA). The latter, roughly speaking, are signature/message authentication schemes where `tags' on multiple messages can be homomorphically combined to yield a `tag' on any linear combination of these messages.We provide a framework for building public-key HLAs from any identification protocol satisfying certain homomorphic properties. We then show how to turn any public-key HLA into a publicly-verifiable PoS with communication complexity independent of the file length and supporting an unbounded number of verifications. We illustrate the use of our transformations by applying them to a variant of an identification protocol by Shoup, thus obtaining the first unbounded-use PoS based on factoring (in the random oracle model).

C. *ODSBR: An on-demand secure by zantine resilient routing protocol for wireless ad hoc networks*

Ah hoc networks offer increased coverage by using multihop communication. This architecture makes services more vulnerable to internal attacks coming from compromised nodes that behave arbitrarily to disrupt the network, also referred to as Byzantine attacks. In this work, we examine the impact of several Byzantine attacks performed by individual or colluding attackers. We propose ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provides resilience to Byzantine attacks caused by individual or colluding nodes. The protocol uses an adaptive probing technique that detects a malicious link after log n faults have occurred, where n is the length of the path. Problematic links are avoided by using a route discovery mechanism that relies on a new metric that captures adversarial behavior. Our protocol never partitions the network and bounds the amount of damage caused by attackers. Our analysis of the impact of these attacks versus the adversary's effort gives insights into their relative strengths, their interaction, and their importance when designing multihop wireless routing protocols.

D. *TWOACK: Preventing selfishness in mobile ad hoc networks*

Mobile ad hoc networks (MANETs) operate on the basic underlying assumption that all participating nodes fully collaborate in self-organizing functions. However, performing network functions consumes energy and other resources. Therefore, some network nodes may decideagainst cooperating with others. Providing these selfish nodes, also termed misbehaving nodes, with an incentive to cooperate has been anactive research area recently. In this paper, we propose two network-layer acknowledgment-based schemes, termed the TWOACK and the S-TWOACK schemes, which can be simply added-on to any source routing protocol. The TWOACK scheme detects such misbehaving nodes, and then seeks to alleviate the problem by notifying the routing protocol to avoid them in future routes. Details of the two schemes and our evaluation results based on simulations are presented in this paper. We have found that, in a network where up to 40% of the nodes may be misbehaving, the TWOACK scheme results in 20% improvement in packet delivery ratio, with a reasonable additional routing overhead.

E. *Short signatures from the weil pairing*

We introduce a short signature scheme based on the Computational Diffie–Hellman assumption on certain elliptic and hyper elliptic curves. For standard security parameters, the signature length is about half that of a DSA signature with a similar level of security. Our short signature scheme is designed for systems where signatures are typed in by a human or are sent over a low-bandwidth channel. We survey a number of properties of our signature scheme such as signature aggregation and batch verification.

IV. PROPOSED SYSTEM

In proposed, we calculate the trust between the nodes. Where the nodes are classified as Unknown, and Known. Trust classification and calculation is made on demand based on the data transfer route request. Based on the results on the previous module, we make trust aware routing module. Where the problem of packet dropping is avoided by making the transmission in the trust aware routing nodes. A selective packet drop is a kind of denial of service where a malicious node attracts packets and drops them selectively without forwarding them to the destination in Fig.2. As an example consider the scenario in Fig.1. Here node 1 is the source node and node 7 is the destination node. Nodes 2 to 6 acts as the intermediate nodes. Node 5 acts as a malicious node. When source wishes to transmit data packet, it first sends out RREQ packets to the neighboring nodes. The malicious nodes being part of the network also receives the RREQ. The source node transmits data packets after receiving the RREP from the destination. As node 5 is also the part of routing path will receive the data packets and drops some of them while forwarding others.

This type of attack is very hard to detect as the malicious nodes pretend to act like a good node. The source selects the shortest and the next shortest path. Whenever a neighboring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions.

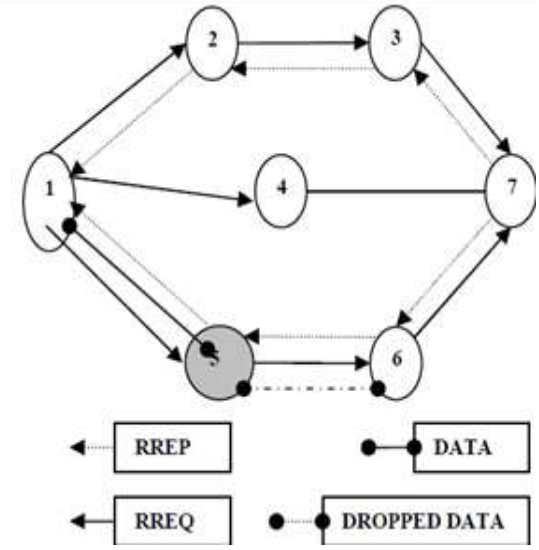

Fig. 1 System architecture

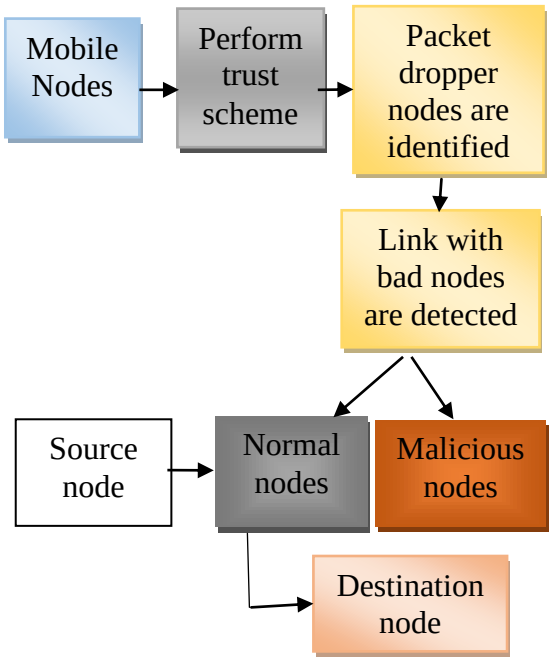

Fig. 2 Block diagram of trust scheme

If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad hoc

network are companions. Further the overheads due to the calculations of trustrelationship are minimal compared to the CONFIDANT protocol. It will be slightly more than the normal DSR due to the invocation of the trust estimator whenever a data transfer is to be done through known or unknown.

V. IMPLEMENTATION AND RESULTS

A. *Direct trust*

Direct trust agent performs the following tasks derivation of trust, quantification and trust computation. Node x want to calculate the trust value on node y termed as

$$dtxy = ps / pr \quad (1)$$

Where dtxy is the final direct trust value of x and y. ps is the successful packet sent from the node x. pr is the successful packet receive from the node y. To calculatethe direct trust on node y, node x has to monitors the statistics. The trust calculation is shown in Fig.3.

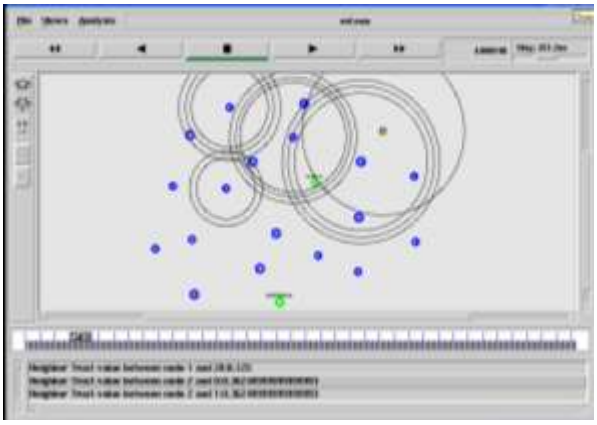

Fig.3 Calculating the trust values of all the nodes

B. *Recommendation trust*

The task of indirect trust monitor is to collect or request the trust related information of target node from the neighboring nodes. The neighbor collecting the trust information is another issue. In other words, while requesting the trust information of the target node from neighbors, the direct trust value of that neighbour node should be considered. This is to avoid the security attacks like bad mouthing. This information generally called as Recommendation trust. Obtaining Indirect Trust on Y from N.

Step 1: Node X sends RTREQ to node(s) N.
Step 2: If node X has direct trust value on Y, then it will reply back with RTREP.

Step 3: Else If X does not have direct trust value record it
will discard the RTREQ
Step 4: After receiving RTREP reply from neighbours consider the trust value of the node with maximum direct trust value by applying fuzzy logic.
Step 5: Integrate all the obtained RT value from neighbours to calculate the indirect trust value.

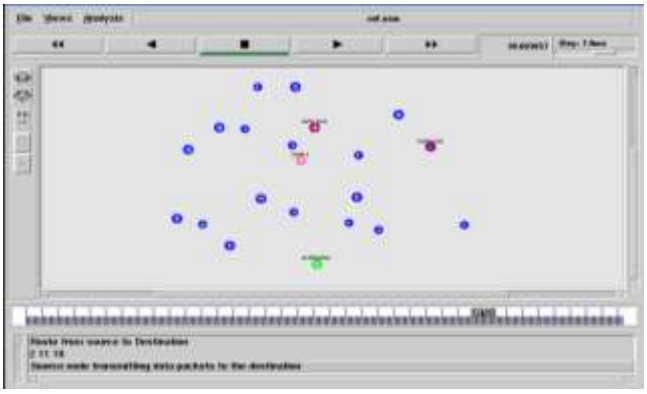

Fig.4 Malicious nodes are detected using trust values

The task of recommendation agent is to collect or request the trust related information of target nodefrom the neighbouring nodes. The source node will broadcast the recommendation request packet toall its neighbouringnodes. From the reply packets, fuzzy logic is applied to the direct trust value of all the replied neighbours. The node with maximum trust value is considered for evaluation of recommendation trust value. By using trust value malicious nodes are detected as shown in Fig.4.

C. *Trust Handler*

The trust handler handles all the incoming and outgoing ALARM messages. Incoming ALARMs can originate from any node. Therefore, the source of an ALARM has to be checked for trustworthiness before triggering a reaction. This decision is made by looking at the trust level of the reporting node. The proposed framework has provisions for several partially trusted nodes to send ALARMs which will be considered as an ALARM for a single fully trusted node. The outgoing ALARMs are generated by the node itself after having experienced, observed, or received a report of malicious behaviour. The recipients of these ALARM messages are called friends, which are maintained in a friends list by each node. The ALARM should be generated even when the Final Trust value is low. Reputation accumulator collects all the information from the Trust Monitor, which is essential to compute the Final Trust Value (FTV) for each node. After Finalizing the Final Trust Value, by holding this value, it could say that, the partial Identification of Malicious node. It was identified by using Trustworthy Mechanism. After identifying the trust, it generates the alarm to its neighbour nodes to avoid

havoc in the network. The trust table maintains the trust records of each node to determine the trustworthiness of an incoming alarm. The friend list contains the list of all nodes to which the node has to send alarms when it detects any malicious activity. Trust evaluator generates a Trust Record Table (TRT) with Node id, trust type and Trust value of each node. Each node maintains a TRT table and every time trust is evaluated TRT table is updated.

FTvalue = Evalue+DTvalue+IDTvalue

Where,

Evalue = Energy value, DTvalue = Direct trust value, IDTvalue = Indirect trust value

Propagation or updating of the trust is done by either reactive manner. In this approach trust is updated only when demanded. So each node contains the direct trust value of all remaining nodes as well as the indirect trust or recommended trust value. Nodes with less trust values marked as MALICIOUS. An alarm is generated by the Trust Manager to indicate the node's malicious behaviour to other trusted nodes in its range thus isolating the less trusted nodes and building a secure system. No suspicious and misbehaving nodes can cause vulnerabilities and threats to the proposed scheme. Trust values of each node are calculated and packet transmission is done through nodes which has highest trust values. By using the highest trust values, the packets are send from source node to destination node through intermediate node as in Fig.5 and Fig.6. These trust values are calculated dynamically time to time and updated. Hence it ensures the secure transmission of packets.

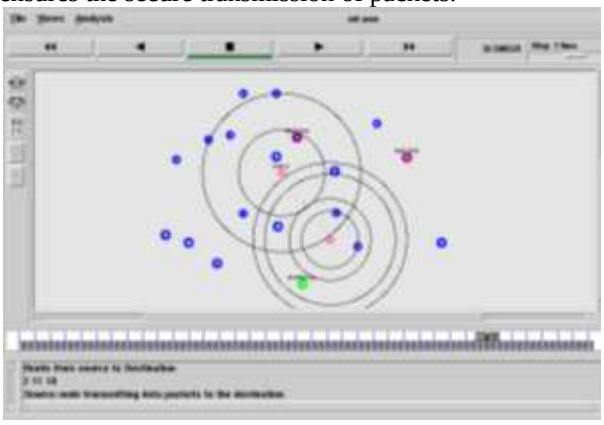

Fig.5 Transmission of packet from source to intermediate node

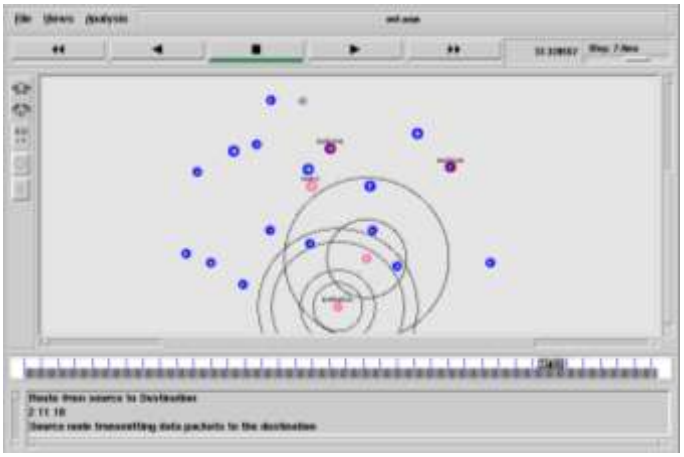

Fig.6 Transmission of packet from intermediate to destination node

VI. PERFORMANCE EVALUATION

A. Packet delivery ratio

In the Fig.7, Packetdeliveryratio_Trust indicates the highest ratio of packets delivered to the destination.

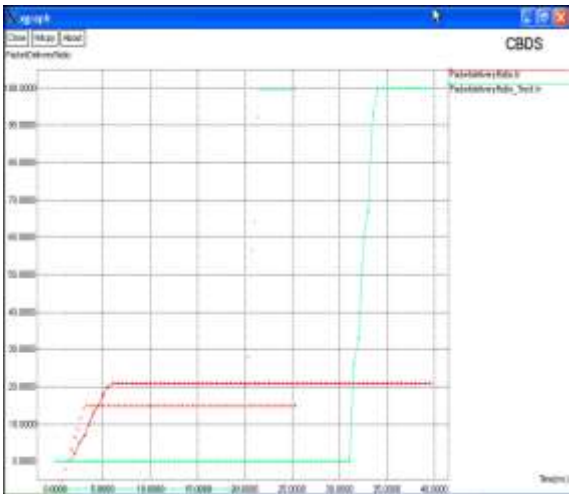

Fig.7 Packet delivery ratio.

B. Packet loss ratio

In the Fig.8, Packetlossratio_Trust shows no loss occurred during the packet transmission.

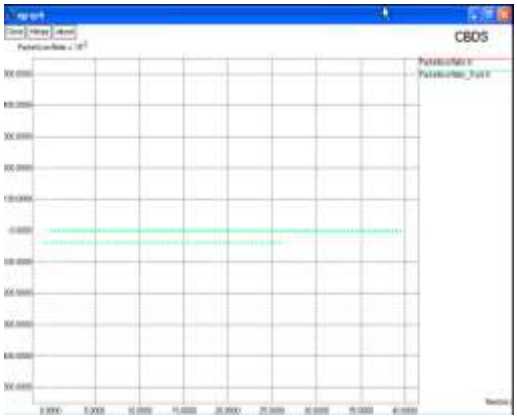

Fig.8 Packet loss ratio

C. *End to end delay*

In the Fig.9, E2Edelay_Trust shows the time duration of packet delivery from source to destination node.

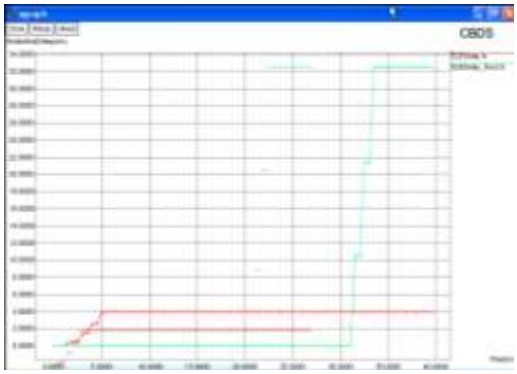

Fig.9 End to end delay

D. *Routing overhead*

In the Fig.10, RoutingOverhead_Trust shows that no change in the packet transmission path. But in the existing system, RoutingOverhead shows the malicious nodes are detected during the packet transmission so it many deviations in the packet transmission path.

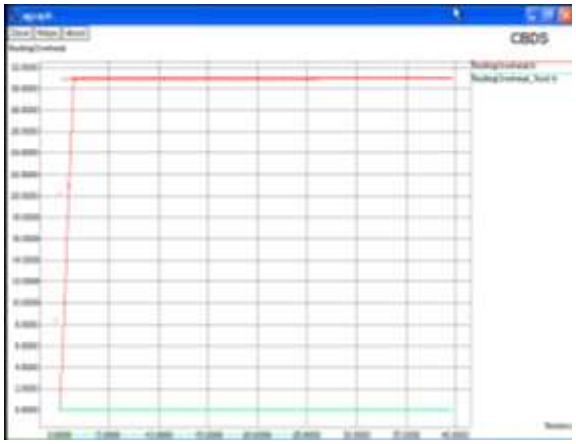

Fig.10 Routing overhead

VII. CONCLUSION

In this research work the solution to calculate the trust in mobile ad hoc network and to identify the malicious nodes taking energy utilization factor as an additional factor in calculating direct trust. Further performance evaluation by simulation and the investigation of additional elaborate adversary models, both for misbehaviour and for trustworthiness, are under way. Various important issues of design of such systems for wireless communication networks are also presented. In future the addition of some watchdog mechanisms for supervisor module will get more secured network. By considering some additional factors like wrong routing, replay packets generated, battery exhaustion, link broken will add more accuracy for the calculation of trust value. By considering the more reasons for packet dropping it will get more accurate trusted network. As a future enhancement this work can be extended to detect the selfish nodes which are malicious and malicious nodes which are acting as selfish nodes.

VIII. REFERENCES

[1] Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE Transactions on mobile computing, Vol. 14, No. 4, April 2015

[2] Sonja Buchegger, Jean-Yves Le Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks", EPFL IC Technical report IC 2003

[3] G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", International Journal of Computer Applications Volume 9– No.9, November 2010 [12] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", ScienceDirect Ad Hoc Networks 1 (2003) pp 13–64.

[4] Yacine Rebahi, Vicente .E Mujica-V and Dorgham Sisalem, "A Reputation-Based Trust Mechanism for Ad hoc Networks", proceedings of IEEE symposium on computers and communications 2005.

[5] Rajan Shankaran, Vijay Varadharajan, Mehmet A. Orgun, and Michael Hitchens, "Critical Issues in Trust Management for Mobile AdHoc Networks", Information Reuse and Integration,IEEE 2009.

[6] Jaydip Sen, "A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks", Computer Research Repository of IEEE 2010.

[7] Hui Xiaa, Zhiping Jiaa, Xin Lia, Lei Jua, Edwin H.-M. Shab, "Trust prediction and trust-based source routing in mobile ad hoc networks", ScienceDirect Ad hoc Networks 6 (2010).

[8] R. Sathish Kumar and S. Pariselvam , "Formative Impact of Gauss Markov Mobility Model on Data Availability in MANET", Asian Journal of Information Technology 11(3): 108-116 ,2012.

[9] Ramprasad Kumawat and Vinay Somani "Comparative Study of On -demand Routing Protocols for Mobile Ad-hoc Network", International Journal of Computer Applications Volume 27– No.10, August 2011.

[10] Vijayan R, Mareeswari V and Ramakrishna K, "Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 3, June 2011 pp 647-652.

[11] Ji Guo , Alan Marshall, Bosheng Zhou, "A New Trust Management Framework for Detecting Malicious and

Selfish Behaviour for Mobile Ad hoc Networks", 2011 International Joint Conference of IEEE.

[12] Manoj V, Mohammed Aaqib ,Raghavendiran N and Vijayan R "A Novel Security Framework Using Trust and Fuzzy Logic in MANET", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[13] Pankaj Sharma and Yogendra Kumar Jain, " TRUST based Secure AODV in MANET", Journal of Global Research in Computer Science Volume 3, No. 6, June 2012..

[14] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610

[15] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319–333.

[16] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

[17] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[18] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.