SMTCI: Secure Multi-Trial Trust Evaluation and Cost- Effective Incentive Mechanism for Multi-Hop Cellular Networks

B.Sumathi[1], V.Hamsadhwani[2]
[1]M.Tech Scholar, Department of Information Technology
Periyar Maniammai University, Thanjavur, Tamil Nadu, India.
[2]Assistant Professor, Department of Information Technology
Periyar Maniammai University, Thanjavur, Tamil Nadu, India.
[1]csesumathi@gmail.com
[2]bellhwk@yahoo.co.in

***Abstract*— In multi-hop cellular networks, finding an optimum and trusted route in the network through intermediate node is a major issue. At MCN, or the next-generation wireless networks, can significantly improve network performance and deployment and help implement many novel applications and services. However, when compared to wired and single-hop wireless networks, MCNs are highly vulnerable to serious security threats because packets may be relayed through integrated networks and autonomous devices. Our Proposed work has been focusing on developing secure trust based protocols for securing MCNs. Specifically, we are interested in securing route establishment and data transmission processes, establishing stable routes, and preserving users' anonymity and location privacy. In this paper we propose a multi-trial trust evaluation scheme, trusted node based ad hoc routing using trials to establish security accomplishes establishment of trusted networks in MANETs. We apply the same idea to develop our proposed algorithm TBARA to rate neighbor nodes using hash values for identifying the misbehaving nodes. After the successful transmission of packets from source to destination, the destination will send acknowledgement for the corresponding packet, upon receiving of acknowledgement incentive will be generated. It reduces the number of public-key cryptographic operations and protect against collusion attack.**

Keyword— Multi-Hop Cellular Networks, Multi-Trial Trust Evaluation, Payment Schemes, Wireless Communication.

I. INTRODUCTION

MULTIHOP cellular network (MCN) [1], [2], [3], [4] is a network architecture that incorporates the ad hoc characteristics into the cellular system. A node's traffic is usually relayed through other nodes to the destination. The network nodes commit bandwidth, data storage, CPU cycles, battery power, etc., forming a pool of resources that can be shared by all of them. The utility that the nodes can obtain from the pooled resources is much higher than that they can obtain on their own. Multi-hop Ad Hoc Networks are collections of multiple nodes connected together over a wireless medium. These nodes can freely and dynamically self-organize into arbitrary and temporary, "ad-hoc" network topologies, allowing devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, (e.g., disaster recovery environments).[5].

A hybrid ad hoc network[6] is a structure-based network that is extended using multi-hop communications. Indeed, in this kind of network, the existence of a communication link between the mobile station and the base station is not required: A mobile station that has no direct connection with a base station can use other mobile stations as relays. Compared with conventional (single-hop) structure-based networks, this new generation can lead to a better use of the available spectrum and to a reduction of infrastructure costs. However, these benefits would vanish if the mobile nodes did not properly cooperate and forward packets for other nodes.

The major idea of MCNs[7] is based on multi-hop relaying. The source node signals are relayed through other intermediate nodes to the Base Station. The intermediate nodes can be fixed, mobile or ad hoc relays. In this way the benefits of an MCN was achieved they are, the capacity can be enhanced, the coverage can be extended, the hot spot and dead spot problems can be alleviated and the radio resource can be better utilized. Based on the multiple hops from the source to destination whether the infrastructure is used or not[8], we can distinguish the two kinds of multi-hop wireless network, Pure ad hoc networks do not rely on any fixed infrastructure; hence, the packet relaying service has to be provided solely by the end user devices.

Multi-hop cellular networks rely on a set of base stations that are connected to a high speed backbone network; [10] here, data packets have to be relayed by end user devices from the source to the backbone and from the backbone to the destination and both types of network requires the end users to collaborate. However, collaboration is not individually beneficial for the users, because it consumes resources such as battery power, memory, and CPU cycles, and it does not provide any immediate advantages Indeed, if the majority of the users collaborate, a selfish user can parasitically take advantage of this by using the network without contributing to it.

In MCN, trust management is a major issues to overcome this issue, Before that we can compare different trust evaluation methods[9] or discuss trust models for ad hoc networks. In existing ad hoc networks, trust relationship can be established in two ways. The first way is through direct observations of other node's behavior, such as dropping packets etc. The second way is through recommendations from other nodes and it also focuses on trustworthiness evaluation process after initial trust relationship has been established. The existing information theoretic framework[9] of trust modeling and evaluation schemes are applied to improve network performance and security of ad hoc routing protocols.

MCN systems will require the cooperation of nodes in relaying other user's data. However, certain users might exhibit a selfish behavior motivated by aspects such as battery exhaustion, traffic overload, technological distrust, or intrinsic selfishness[10]. To incentive nodes to cooperate in network functions, and prevent intentional attacks from malicious nodes, Our Proposed work has been focusing on developing secure trust based protocols for securing MCNs. Specifically, we are interested in securing route establishment and data transmission processes, establishing stable routes, and preserving user's anonymity and location privacy. They are several incentive mechanism have been proposed for make use of cooperative nodes but we applying a fair incentive mechanism[20] with trusted network, by establishing a trusted route we use a multi-trial trust evaluation scheme, trusted node based ad hoc routing using trials to establish security accomplishes establishment of trusted networks in MANETs. We apply the same idea to develop our proposed algorithm TBARA to rate neighbor nodes using hash values for identifying the misbehaving nodes. and then fair incentive mechanism can be applied for stimulating the selfish nodes, Extensive analysis identifies the trusted route throughout the network. finally the simulation results shows that the overhead of the proposed mechanism is incomparable with the existing one.

II. RELATED WORK

In MCNs, cooperation enforcement schemes are seen as a viable, lightweight alternative to conventional security techniques involving cryptographically signed certificates exchange, providing a “softer” security layer to protect basic networking operations. Cooperation enforcement schemes[11] fall within two broad categories: trust establishment by means of reputation systems and pricing and credit-based schemes. The first category is based on building reputation of nodes, while the second provides for economic incentives.

Reputation-based schemes utilize reputation in routing [12] and/or enforcing punishment[13]. However, the existing reputation-based schemes suffer from lack of effective mechanisms to measure and propagate reputation. Without quantitative and objective ways to measure reputation, and secure ways to propagate reputation, a reputation-based incentive scheme would not serve the purpose of stimulating packet forwarding, since reputation can be easily manipulated by selfish nodes in this case. Hence, this mechanism proposes a quantity to objectively measure reputation of a node, and a secure mechanism to propagate reputation, with the aim of resolving the drawbacks of the existing reputation-based incentive schemes.

Credit-based schemes consider packet forwarding as a market model where nodes providing a service are remunerated, whilst nodes receiving a service are charged. Hence, if a node wants to send its own packets, it must forward packets for the benefit of others. However, these Cooperation stimulation mechanisms can be classified as: tamper-proof device (TPD) based, central bank based and electronic coins based mechanisms. In the TPD based mechanisms[18], a tamper-proof device (which cannot be tampered) is installed in each device to store its credits and to secure its operation. In the central bank based mechanisms[14], a centralized accounting center (AC) stores and manages the nodes’ accounts. The nodes periodically send receipts resulted from their cooperation activities to the AC to update their accounts or infrastructure-dependent credit clearance systems [19]that other nodes can trust.

In Sprite [14], an intermediate node stores a receipt from each relayed packet. When it has a fast connection to the accounting centre, the node transmits the receipts. A significant communication overhead is implied because the number of claimed receipts is large due to generating a receipt for each packet. In [16], a technique is introduced to generate a receipt for multiple packets but the authors did not show how it can be implemented efficiently in a routing protocol. They also did not use simulations to evaluate it. In [17], the sender appends a signature to the full path identities and an initialization of a keyed hash chain. Each intermediate node verifies the signature and computes a new hash value using the attached hash value. The recipient generates a receipt of the received amount of data, and sends it to the last intermediate node to transmit

to the accounting centre. Two colluders can communicate for free by exchanging packets with invalid hash value because the intermediate nodes cannot verify it.

In Express [29], the source node generates a hash chain for each intermediate node ID_K and commits to the hash chain by digitally signing the root of the hash chain and sending the signature to ID_K. Each time the node ID_K relays a message, the source node releases the pre image of the last sent hash value. The source, intermediate, and destination nodes compose checks and submit them to the AC. However, the nodes have to generate and store a large number of hash chains because any node in the network may act as an intermediate node due to the node mobility. The packet overhead is large especially if the number of intermediate nodes is large because the source node attaches one hash value for each intermediate node.

In Nuglet [15] cooperation scheme, Every time a node wants to transmit a self-generated packet, it has to pay with Nuglet. the below Fig.1 shows that example of Nuglet Scenario. The amount corresponds to the estimated number of nodes between the sender and receiver (intermediate nodes). Every time a node forwards a packet it receives one Nuglet.

Reputation-based and incentive mechanisms [24], [25] have been proposed to thwart selfishness attacks. For reputation-based mechanisms [21], [22], [23], the nodes usually monitor the transmissions of their neighbors to make sure that the neighbors relay other nodes' traffic, and thus, selfish nodes can be identified and punished. For incentive mechanisms, packet relay is a service not an obligation. The source and destination nodes pay credits (or virtual currency) to the intermediate nodes for relaying their packets. Credits can stimulate the node's cooperation by proving that it is more beneficial for the nodes to cooperate than behaving selfishly.

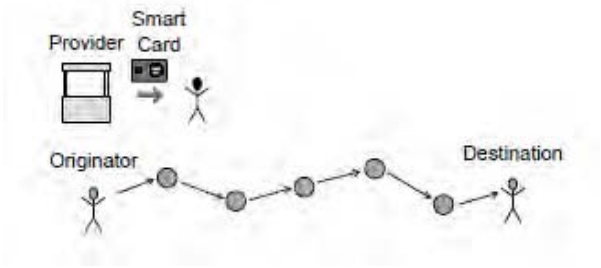

Fig.1. Example of Nuglet Scenario

The existing reputation based mechanisms[20] has several disadvantages when implementing them in MCN.

-Monitoring the nodes' transmissions by overhearing the channel is not energy efficient for transmitters..

-Reputation-based mechanisms do not achieve fairness because the highly contributing nodes are not compensated.

-The mechanisms suffer from unreliable detection of the selfish nodes and false accusation of the honest nodes. That is because it is difficult to differentiate between a node's unwillingness and incapability to cooperate, e.g., due to low resources, packet collision, and network congestion.

In order to overcome the above disadvantage, we propose a multi-trial trust evaluation scheme, trusted node based ad hoc routing using trials to establish security accomplishes establishment of trusted networks in MANETs. We apply the same idea to develop our proposed algorithm TBARA to rate neighbor nodes using hash values for identifying the misbehaving nodes at the route discovery phase and to establish the stable routes, Stable routes are established through the evaluated trusted nodes having sufficient energy and then FESCIM[20] mechanism can be applied for stimulating the selfish nodes, and to secure the payment, trust calculation and significantly improve route stability and thus the packet delivery ratio.

III. System Architecture

A. Network and Communication Model

The Fig.2. shows that the architecture of the multi-hop cellular network, includes an Accounting centre(AC), several Base Station(BS) and several Mobile Nodes(MN). The architecture of the MCN in this paper was specially designed for the trusted route establishment within the base station coverage area and it prevents from thwart selfishness attacks for example denial of service attacks, flooding attacks etc., we propose a multi trial trust evaluation scheme in the route discovery phase, In this phase we use a TBARA algorithm to establish the trusted route and to identify the Selfish Nodes(SN) and Trusted Nodes(TN) in a network. each base stations are connected with each other and the Accounting Centre(AC) by a backbone network that may be a wired or wireless network. we assume our proposed algorithm TBARA use the Ad-hoc on demand Distance Vector (AODV) routing protocol to establish an end-to-end communication.

All communications are unicast[20] and the nodes can communicate in one of two modes: pure ad hoc or hybrid. For pure ad hoc mode, the source and destination nodes communicate without involving base stations. The source node's messages may be relayed in several hops by the intermediate nodes to the destination node. For hybrid mode, at least one base station is involved in the communication. The source node transmits its messages to the source base station (BS_S), if necessary in multiple hops. If the destination node resides in a different cell, the messages are forwarded to the destination base station (BS_D) that transmits the messages to the destination node possibly in multiple hops. The nodes can contact the AC at least once every few days. This connection can occur via the base stations or the wired networks such as the Internet. During this connection, the nodes submit checks, renew their certificates, and convert credits to real money and/or purchase credits with real money.

AODV [26] is a reactive routing protocol that only searches and establishes a route when the source has information to transmit and does not know the route to reach the destination node; therefore overall network information is not required unlike proactive protocols. In this case, the source node sends a broadcast Route REQuest (RREQ) message that is retransmitted by neighboring nodes. When the destination node receives the RREQ message, it replies with a unicast Route REPly (RREP) message to confirm the route establishment. The reception of RREQ and RREP messages allow intermediate nodes to know their neighboring nodes in the route towards the source and destination nodes.

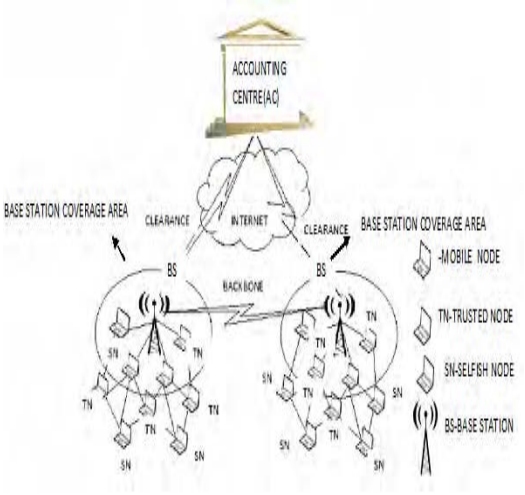

Fig.2. The architecture of the Multi-Hop Cellular Network

IV. OVERVIEW OF THE PROPOSED SYSTEM

The design of multi-trial trust evaluation systems focuses on establishing trust with high accuracy and low overhead, and on utilization of trust values to improve security and network performance. To the best of our knowledge this is the first time in this paper, we propose a multi-trial trust evaluation schemes in a cooperative networks to detect the selfish node and untrusted node at the initial step of route discovery phase and we use a TBARA algorithm to establish the trusted route and by applying the cryptographic mechanism enables already authenticated message to connect to a trusted nodes. second, the packet transmission can be processed from the source node to the destination node through the trusted nodes and acknowledgment can be received for every packet. Based on the acknowledgment the small size check can be generated per group of packets and the incentive can be provided based on the successful submission of checks to the accounting centre.

A. Multi-Trial Trust Evaluation Scheme:

Trusted node based Ad hoc routing using Trials to Establish Security accomplishes establishment of trusted net-works in ad hoc networks in the same way as in real life scenarios. We apply the same idea to develop our proposed algorithm TBARA. The proposed TBARA algorithm is divided into the following four Stages:

1. Test your neighbor,
2. Rate neighbor nodes,
3. Share Benign node,
4. Route through other trusted nodes,
5. Maximize the credits.

The Fig.3 also depicts the link/flow between the different stages of the algorithm. The routing of data in the protocol is on demand; that is whenever the need arises. But challenges, trusted node sharing and rating are periodic processes. This makes the TBARA protocol a hybrid one.

The Test your neighbor stage is designed to facilitate trust establishment for a new node in relation to the other nodes present in the network. Rate trusted nodes, Share trusted nodes and Route through trusted nodes gradually make the network robust in terms of the reliability of the nodes, and it is through these stages that the nodes gather data about each other and populate a trusted list where the information about reliable nodes is kept. A node having its neighbors in its trusted list does not need to challenge them before a data session.

B. Trust Based Ad hoc Routing Algorithm(TBARA):

The algorithm supports the management of trust and fairness by allowing nodes to publicly declare that they refuse to forward messages to some nodes[27] .

Each node ***A*** maintains some variables to evaluate the trust,

$trusted_A$: The set of nodes to which A is willing to provide services.

$untrusted_A$: The set of nodes to which A is not willing to provide services.

$selfish_A$:The set of nodes which are trustworthy by A.

$neighbor^B$: The set of nodes to which B is to facilitate the trust establishment to the other nodes A & C. For each other known node *B*, node *A* will keep a number of status variables, as follows:

$trusted_A^B$:The set of nodes for which *B* is willing to provide services. This set is initialized with every node known by node *A*.

$untrusted_A^B$:The set of nodes to whom *B* is known not to provide services. A node *C* can be inserted in this set either because *B* explicitly advertises *C* as its untrusted or because *C* declares *B* to be selfish. This set is empty when initialized.

$liedTo_A^B$:A set of nodes to which *B* is known not to provide services, even though it had advertise them as trusted nodes. The set $liedTo^B_A$ is always a subset of $untrusted^B_A$.

$encrypted\ hashchain_A^B$: The security of an encrypted hash depends on the security of the hash chain function, and, of course, on the size and the quality of the key, the destination node generates a hash chain with the size of Z+1 by iteratively hashing a random variable called seed(H_D^0(i))Z times to obtain a final hash value called root (H_D^Z(i)),where $H_D^X(i)=H(H_D^{X-1}(i))$ and i is the hash chain number .

MAC_A^B: Assuming a collision-resistant hash function, the original message and its MAC(Message Authentication Code) can be safely transmitted over a network without worrying that the integrity of the data may get compromised.[28]. A recipient with access to the key used for calculating the message(data packet)can verify the integrity of the message by recomputing its MAC and comparing it with the value received. The function that generates the MAC of a message(data packet) M using a secret key K by C(K,M).

$$MAC=C(K,M)$$

$msgpending_A^B$: The set of messages forwarded by *A* to *B* waiting to be acknowledged.

$msgsuspected_A^B$:An unsigned integer increased for each message forward by *A* to *B*, but whose forwarding by *B* was not listened by *A* (e.g. due to collisions).

$deadbeat_A^B$**:** An unsigned integer that will be set to zero whenever a message is listen from *B*. Periodically, a timer will increase this value. If it reaches some threshold, one can consider that the node is no longer in the neighborhood.

$relay_A^B$:Assuming that the relay nodes serves as a repeaters, they receive and transfer to other node D

$credits_A^B$**:** A signed integer increased for each message that *A* forwarded on behalf of *B* and decreased for each message that *B* sent on behalf of *A*. The initial value is 0.

$maxcredits_A^B$:The upper bound to $credits^B_A$, the maxcredits can be transfered to the AC in the form of check.

In our MCN, it is acceptable for some of the intermediate nodes are act as a selfish nodes, it cannot relay the other nodes. To evaluate if the number of untrusted nodes declares an unacceptable level of selfishness. each node A advertises the content of these three variables in a control message[28] with the following format:

SELFSTATE[*A,*| $trusted_A$, $untrusted_A$,| *selfishA]*

In order to evaluate the degree of selfishness of other nodes, and to detect inaccuracies in the information advertised by other nodes, each node keeps a record of received SELFSTATE.

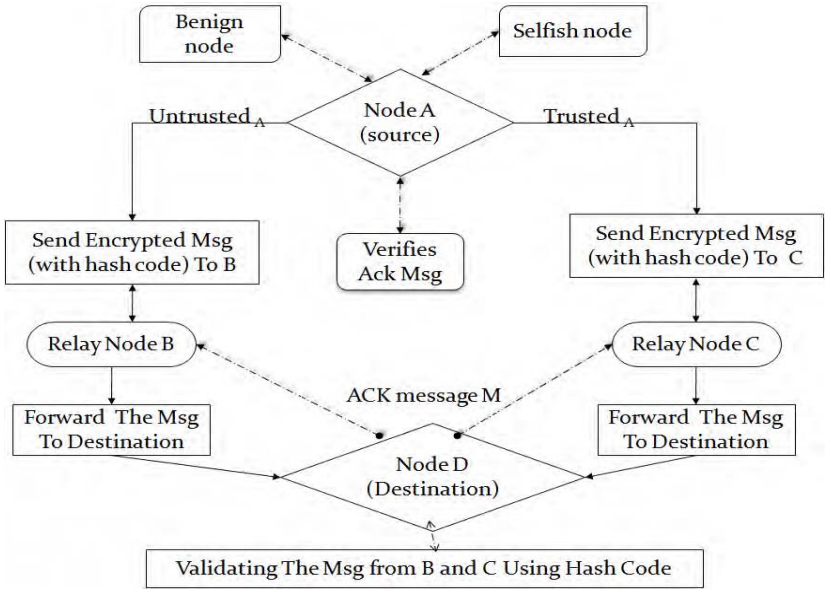

Fig.3. Flow Diagram for TBARA Algorithm

C. Check Generation:

For each route, one check containing the payment data for all the intermediate nodes can be composed. The general format of the route check contains the session identifier S_i, identity of the source(ID_S) and the identity of the destination(ID_D) and the number of successful acknowledgment received(ACK_R) and also contains the message number(X), Security Token(S_t) the hash value of the last received messages, and the last released hash value ($[H_D^{Z-L}(V)]$) , The Security Token(S_t)[20] is an undeniable proof that prevents payment repudiation and manipulation, and thus ensures that the check is undeniable, unmodifiable, and unforgeable. In order to significantly reduce the check size, the security token is composed by hashing the source and destination nodes encrypted message instead of attaching the large-size signature. The check size depends on the number of used hash chains because two hash values should be attached for each hash chain, and thus properly choosing the hash chain size can minimize the check size.

D. Check Clearance:

The base station submits the check to the AC for redemption, but the nodes submit the check[20] if the base station belongs to a different operator. The nodes also submit the check if the route is not complete, i.e., the EOS packet is not received, and the base station does not have correct payment information. For example, if the route is broken during relaying the ACK of Message M from the destination BS_D, the BSD's check does not prove that the X^{th} message is delivered, and thus, the nodes are not rewarded for the last message if they do not submit the check. Once the AC receives a check, it checks that the check has not been deposited before using its unique identifier (Si). Then, the AC generates the source and destination node's signatures and hashes them to verify the check's credibility. The check is valid if the resultant hash value is identical to the check's Security Token. For a check (C(x)), the number of transmitted messages (X) is signed by the source node, and the number of delivered messages can be computed from the number of hashing operations to map $H_D^{Z-X}(1)$ to $H_D^Z(1)$.

V. Simulation Results

In our simulation, we use Network Simulator NS2(version 2.28) In the simulation 300 nodes are randomly distributed within the network field of size 1000m*1000m. Then vary the node speed from 5m/s to 30m/s. Network Simulator NS2 is used to evaluate the average trust value and the network throughput using hash chain based ACKs. The constant bit-rate traffic source is implemented in each node of an application layer. The source and destination pairs are randomly selected. we stimulate the ad hoc on demand distance vector (AODV) routing protocol[26] each node has its own encryption key and node identity number and also each time simulation session starts, it is identified by the unique session identifier S_i. A few seconds after the simulation starts, a node can randomly assumed their channel head(CH) and access point(AP) in the network simulation. In our simulation we use SHA-1 hash function[20] to reduce the acknowledgement and to establish the trusted route. Every time the node transmits a data packets from the source to destination through the access point (AP), In access point(AP) our proposed algorithm TBARA algorithm can be implemented and to finalize their routing path based on the TBARA algorithm steps and through the trusted node establishment.

The Fig.4 shows that the Average Trust value of the nodes, the average trust value is gradually

increases when the number of nodes also increases slowly, when the average trust value tends to be stable, the number of nodes is increases slowly and the proposed TBARA algorithm analysis and maintains the trust value to establish the routing process. In MCN, we observed that the number of nodes in a network and change their transmission power randomly, some of the node act as selfish nodes it degrades the performance of the network. we evaluate the trust value of the nodes by applying TBARA algorithm, Fig.5. shows that comparison of Node vs. trust value of nodes the performance evaluation of the nodes decreases gradually with the increases of trust value of nodes. If the trust value of nodes is high, then the probability distribution of an node capacity is also high, and data transmission through the trusted nodes that increases the throughput.

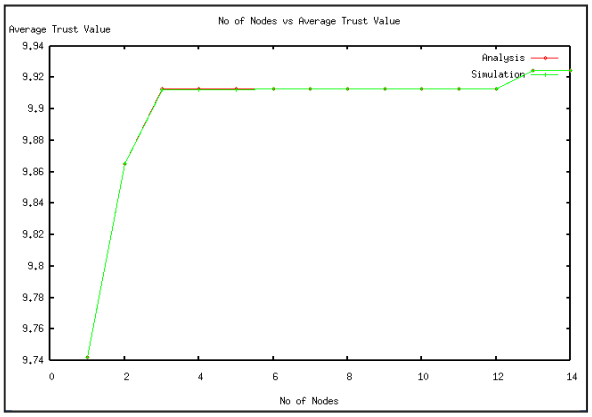

Fig.4. The Average Trust Value of the Nodes

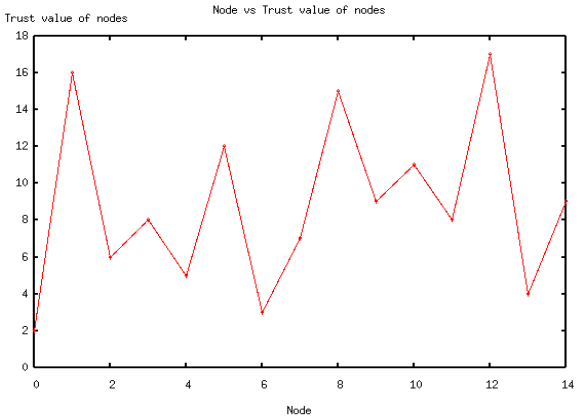

Fig.5. Comparison Between The Node Vs Trust Value Of Nodes

VI. CONCLUSION

This paper concludes that the proposed multi-trial trust evaluation systems focuses on establishing trust with high accuracy and low overhead. In a cooperative networks to detect the selfish node and untrusted node at the initial step of routing process and TBARA algorithm must establish the trusted route, and the check can be composed. some of the critical issues in trust establishment in multi-hop cellular networks include the protection of incentive information and to reduce the lightweight signature key distribution schemes our proposed algorithm overcomes such issues and on utilization of trust values to improve security, average trust value of node increase the throughput and network performance.

REFERENCES

[1] Lin and Y. Hsu, “Multihop Cellular: A New Architecture for Wireless Communications,” Proc. IEEE INFOCOM, vol. 3, pp. 1273-1282, Mar. 2000.
[2] X. Li, B. Seet, and P. Chong, “Multihop Cellular Networks: Technology and Economics,” Computer Networks, vol. 52, no. 9, pp. 1825-1837, June 2008.
[3] C. Gomes and J. Galtier, “Optimal and Fair Transmission Rate Allocation Problem in Multi-Hop Cellular Networks,” Proc. Int’l Conf. Ad-Hoc, Mobile and Wireless Networks, pp. 327-340, Aug. 2009.
[4] H. Wu, C. Qios, S. De, and O. Tonguz, “Integrated Cellular and Ad Hoc Relaying Systems: iCAR,” IEEE J. Selected Areas in Comm., vol. 19, no. 10, pp. 2105-2115, Oct. 2001.
[5] Jon crowcraft, Andrea Passarella, “ Multi-hop ad hoc networks from theory to reality-book ” macro conti (Inst for informatics and telematics,pisa italy) .
[6] Naouel Ben Salem, Levente Buttyán , Jean-pierre Hubaux, Markus Jakobsson " Node cooperation in Hybrid ad hoc networks " IEEE Transactions on Mobile Computing, 2006.
[7] Yik Hung Tam " Resource management in multi hop cellular networks " University Kingston, Ontario, Canada January 2009.

[8] L.Buttyan,M.Jackobsson,J.P.Hubaux, N.B.Salem," Incentive Mechanism in Multi-hop wireless networks "
[9] Yan Sun, Wei Yu, Zhu Han, and K. J. Ray Liu," Trust Modeling and Evaluation in Ad Hoc Networks "
[10] Javier Gozalvez, Baldomero Coll-Perales, Alberto Rodriguez-Mayol and Maria del ," Multi-Hop Cellular Networks based on Mobile Relays: Capabilities and EnablingTechnologies"IEEE COMSOC MMTC, Vol.6, No.3, March 2011.
[11] L. Santhanam, B. Xie, and D.P. Agrawal, "Selfishness in mesh networks:wired multihop MANETs," *IEEE WirelessComm. Magazine*, Vol 15, No 4, August 2008, pp. 16-23.
[12] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proceedings of Mobicom 2000*, Boston, MA, USA, Aug. 2000.
[13] S. Buchegger and J. Le Boudec, "Performance analysis of the CONFIDANT protocol: cooperation of nodes - fairness in distributed ad-hoc networks," *IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, Switzerland, June 2002.
[14] Zhong, S., Chen, J., & Yang, Y. R. (2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. *IEEE Infocom*, *3*, 1987–1997.
[15] L. Buttyan, and J. Hubaux, "Nuglets: A Virtual Currency to Stimulate Cooperation in Self Organized Ad Hoc Networks" , Technical Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne, January 2001.
[16] M. Mahmoud, and X. Shen, "DSC: Cooperation Incentive Mechanism for Multi-Hop Cellular Networks" , Proc. of IEEE ICC' 09, Dresden, Germany, June 14-18, 2009.
[17] B. Lamparter, K. Paul, and D. Westhoff, " Charging Support for Ad Hoc Stub Networks" , Journal of Computer Communications, Vol. 26, No.13, pp. 1504–1514, 2003.
[18] A. Weyland and T. Braun, "Cooperation and accounting strategy for multi-hop cellular networks", Proc. of IEEE Workshop on Local and Metropolitan Area Networks (LANMAN), pp. 193-198, Mill Valley, CA, USA, April 25-28, 2004.
[19] A. Weyland, "Cooperation and accounting in multi-hop cellular networks", Ph.D. thesis, University of Bern, November 2005.
[20] Mohamed M.E.A. Mahmoud, and Xuemin (Sherman) Shen," FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks" ieee transactions on mobile computing, vol. 11, no. 5, may 2012
[21] C. Song and Q. Zhang, "OMH-Suppressing Selfish Behavior in Ad Hoc Networks with One More Hop," Mobile Networks and Applications, vol. 14, no. 2, pp. 178-187, Feb. 2009.
[22] D. Djenouri and N. Badache, "On Eliminating Packet Droppers in MANET: A Modular Solution," Ad Hoc Networks, vol. 7, no. 6, pp. 1243-1258, Aug. 2009.
[23] G. Bella, G. Costantino, and S. Riccobene, "Evaluating the Device Reputation Through Full Observation in MANETs," J. Information Assurance and Security, vol. 4, no. 5, pp. 458-465, Mar. 2009.
[24] J. Hu, "Cooperation in Mobile Ad Hoc Networks," Technical Report TR-050111, Computer Science Dept., Florida State Univ., Jan. 2005.
[25] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation Enforcement Schemes for MANETs: A Survey,"J. Wireless Comm. and Mobile Computing, vol. 6, no. 3, pp. 319-332,2006.
[26] Baldomero Coll-Perales and Javier Gozalvez," Energy Efficient Routing Protocols for Multi-Hop Cellular Networks *Ubiquitous Wireless Communications Research Laboratory, Uwicore, http://www.uwicore.umh.es*
[27] Hugo Miranda Lu´ıs Rodrigues," Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks"
[28] Avi Kak" Hashing for Message Authentication" Lecture Notes on "Computer and Network Security" March 8, 2013.
[29] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. Fallah, "A Secure Credit-Based Cooperation Stimulating Mechanism for MANETs Using Hash Chains," Future Generation Computer Systems, vol. 25, no. 8, pp. 926-934, Sept. 2009.