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

Improved Exponential Reliability Coefficient Based Reputation Mechanism for Isolating Selfish Nodes in Mobile Ad hoc Network

Daniel Nesa Kumar C[1*], Saravanan V[2]

[1]Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore, India
[2] Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, India

[*]*Corresponding Author: danielnesakumar@gmail.com, Tel.: +91-9894255269*
Available online at: www.ijcseonline.org

Accepted: 07/Jun/2018, Published: 30/Jun/2018

***Abstract*—**Mobile Ad hoc Network (MANET) is outstanding for its restricted transmission scope of remote system interface. Thus, multiple hops (multi-hops) might be required for trading the data starting with one node then onto the next over the system with no base stations or switches. In MANETs, as there is no chain of command among nodes, each node is in charge of sending packets to its neighboring nodes. Because of serious asset requirements like memory, registering power, vitality, data transfer capacity and time, a few nodes may not partake in sending the packets for sparing its assets. The nearness of selfish behaviour among nodes may prompt system apportioning and has a noteworthy negative effect in throughput and the system activity. To maintain a strategic distance from such circumstances selfish node deduction is imperative. The proposed framework introduced an Improved Exponential Reliability Coefficient based Reputation Mechanism (IERCRM) which disengages the selfish nodes from the steering way in view of Enhanced Exponential Reliability Coefficient (EExRC). This unwavering quality coefficient controlled through exponential disappointment rate in light of moving normal strategy features the latest past conduct of the versatile nodes for measuring its validity. From the reenactment comes about, it is apparent that, the proposed IERCRM approach outflanks the current Exponential Reliability Coefficient based Reputation Mechanism in terms of performance evaluation metrics such as end to end delay, throughput and detection rate.

***Keywords*—**Manet, Enhanced Exponential, Reliability, Coefficient, selfishnode and Priority Factor

I. INTRODUCTION

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links.

MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omni-directional (broadcast), highly-directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network

Security is a noteworthy worry in the specially appointed systems administration measures, Gagandeep et al., (2012) [6]. Information change in impromptu system must be done in a secured way. The security issue in impromptu system is dynamic topology, data transfer capacity, little gadget size and restricted battery life. Because of the dynamic nature, it is hard to keep up secured transmission in the system, Papadimitratos and Haas, (2002) [7]. The impromptu system does not rely upon any prior foundation with the goal that the node can leave

and join the system in such a circumstance where security may tumble down

An entity mobile node may effort to advantage from other nodes, but declines to share its own resources. Such nodes are called selfish or mischievous nodes and their activities are termed selfishness or misbehavior. Deliberately uncooperative behavior (misbehavior) may outcome in a total communication breakdown [8]. A node may behave selfishly by agreeing to forward the packets and then failing to do so due to Overloaded, Selfish, Malicious or Broken. Behavior node models Collaborative model: A node that behaves properly executing both packet forwarding and routing functions. Selfish node that misbehaves to save its battery life. This node could disable packet forwarding and/or routing functions

The rest of the paper is organized as follows: a brief review of some of the literature works in Manet security is presented in Section 2. The proposed methodology for selfish nodes detectionis detailed in Section 3. The experimental results and performance analysis discussion is provided in Section 4. Finally, the conclusions are summed up in Section 5.

II. LITERATURE SURVEY

In (Tan et al 2012) is proposed an on-demand routing protocol for selecting a route that is dependent on the maximization of the minimum node battery power and reducing the total transmission power necessary for reaching the destination. Moreover, the routing protocol is capable of restricting the control packet flooding during times of route discovery and pre-empts the link failures due to node mobility. First, a power and mobility aware optimization issue is devised. For a real practical deployment, this research work renders a heuristic mechanism, referred to as Power and Mobility Aware Routing (PMAR) protocol. It is observed to be energy efficient, with the potential in controlling the control packet flooding and capable of considerably reducing the network overheads resulting due to link failures. But it faces challenges with optimal shortest path routing selection [9].

In Michiardi et. al [10], the technique detects selfish nodes and forces them to cooperate as well. Similar to CONFIDENT, This technique is based on monitoring system and reputation system, which includes both direct and indirect reputation from the system. Sometimes nodes do not misbehave intentionally; for example when their battery is low, they should not be considered misbehaving nodes and be fired from the network. To do so, the reputation should be rated based on past reputation, which is zero (neutral) at the beginning. In addition, participation in the network can be categorized into several functions such as routing discovery (in DSR) or forwarding packets. The difference between CORE and CONFIDANT is that CORE only allows positive reports to pass through but CONFIDANT allows the negative ones. This means that CORE prevents false reports, and thus it prevents a DOS attack which CONFIDANT cannot do. When a node cannot cooperate, it is given a negative rating and its reputation decreases. In contrast, a positive rating is given to a node from which a positive report is received and then its reputation increases.

Confidant stands for Cooperation of Nodes Fairness in Dynamic Ad-hoc Network .Its aim is to detect and isolate selfish nodes thus making it unattractive to deny cooperation. Main components of Confidant are The Monitor, The Trust Manager, The Reputation System and the Path Manager. In Monitoring the nodes keep a watch on the neighbor nodes by either listening to their transmission or by observing their routing behavior. The trust manager handles the incoming and outgoing ALARM messages and sends ALARM messages to other nodes to make them aware about the malicious nodes. The node themselves make active messages when they encounter, watch or get a report of some pernicious conduct. The notoriety framework comprises of a table which has passages for nodes and their rating and a node is just considered as pernicious if there adequate confirmation about its malevolent conduct. The elements of Path chief incorporates way re-positioning as indicated by notoriety of the nodes in the way, activity on getting a demand for a course from a noxious node, erasure of ways containing vindictive node [11].

Tarag Fahad and Robert [12] Askwith have designed the new mechanism called Packet Conservation Monitoring Algorithm (PCMA) to detect selfish nodes in the presence of partial dropping when the selfish node does not drop all packets but sends some of them and drops other in MANET. Much of research on security policies focuses on policy representation and evaluation or building security mechanisms based on specific policies without addressing policy enforcement.

Jian-Ming Chang et. al [13] designed Cooperative Bait Detection Scheme (CBDS) which is able to notice and prevent spiteful nodes launching cooperative black hole attacks. It incorporates with the proactive and receptive barrier structures and the source node arbitrarily participates with a stochastic contiguous node. At the point when source node starts Route Discovery, it conveys the bait RREQ' and afterward source node gets RREP. In the event that RREP is from not existed goal node or intermediate node then trace which node sends back the RREP according to RREP packet's Record address field. The area of black hole node is listed in the black hole list and observed all other nodes to cancel the certificates of black hole by spreading Alarm packets through the network. Disregard any responses from black hole.

III. PROPOSED METHODOLOGY

3.1 Network model

A collection of mobile nodes are having a distinctive uniqueness, which are associated in an ad hoc environment. The MANET considered as an undirected graph G =(N,P), where N is a group of mobile nodes and P is represented collection routes between mobile nodes. In order to achieve the idea of identifying and removing selfish mobile nodes, the subsequent key points are considered. Originally, the quantity of energy obsessed by each and every mobile node is measured as predictable energy metric of that node for discovering Type I and Type III selfish nodes. Then, the packet delivery ratio of each mobile node is influenced in terms of Exponential Reliability Coefficient through exponential distribution for detecting Type I selfish nodes. Then, Type III selfish nodes are detected while the computed energy metric fall lower than the energy threshold value necessary for a mobile node to be in supportive mode. Lastly the detection of Type I selfish nodes from the energetic steering path is computed based on the investigation of both computed energy metric and exponential reliability coefficient for allowing reliable data distribution. The ERCRM is a distributed method for extenuating selfish nodes in which the reliability coefficient is determined in each and every mobile node rather than a centrallized node.

3.2 Detection of Type I and Type III selfish nodes based on estimated energy metric (E_{est})

When a source node transmit the packets to the target node according to one-hop neighbors, the computed Energy scheme find out the energy range of the middle nodes in the routing path by including the two parameters into account viz.,

(a) The residual power (Rp): It is represented as the quantity of energy originally obtainable in the mobile node before connection establishment.

(b) Power drain rate (Pdr): It is represented as average loss of energy due to the packet forwarding that happens in a variety of sessions.

Hence, the power drain rate of a mobile node can be influenced by including the loss of energy due to data forwarding in a two consecutive session say ‘s’ and ‘s-1’ utilizing exponential weighted moving average technique given by (1)

$$P_{dr} = \alpha \times P_{dr}(s) + (1- \alpha) P_{dr}(s-1) \quad (1)$$

Where,

α – Weighted average

The weighted average is determined through the ratio of least amount of energy (min energy req) necessary for forwarding data in a précised routing path to the least number of hops (min hops) obtainable among the source and destination given by (2)

$$\alpha = (\text{min energy req})/(\text{min hops}) \quad (2)$$

The estimated energy metric (E_{est}) of a mobile node is defined as the ratio of remaining energy of a mobile node to the energy exhaust rate at some instant of time ‘t’ as given by (3)

$$E_{est} = \frac{R_P}{P_{dr}} \quad (3)$$

While the estimated energy (E_{est}) of a node is computed to be lower than the value of Energy threshold is determined as the least amount energy necessary for a mobile node to contribute in the routing action. Then, the mobile node is chosen as selfish.

The following algorithm 1 illustrates the steps to estimate the Estimated Energy Metric (Eest) for each and every mobile node participating in the routing activity and further, from the estimated value of Eest, the behaviour of the node is categorized either as Type I or Type III selfish.

Algorithm 1: (Exponential Reliability Coefficient)

Algorithm (Estimation Energy Metric)
1. For every mobile node n_i in Network N,
2. if $n_i \in$ Routing path (S, n_1,…., n_m, d)
Set Rp ← Energy (n_i), otherwise Rp← 0
3. Calculate , the weighted average αas $\frac{E_{min}}{H_{min}}$
4. Calculate Power Drain Rate through
$P_{dr} = \alpha \times P_{dr}(s) + (1- \alpha) P_{dr}(s-1)$
5. Calculate the Estimated Energy Metric as
$E_{est} = \frac{R_P}{P_{dr}}$
6. if ($E_{est} < E_{thr}$)
Allocate every node n_i (selfishness) ← true; otherwise
n_i (selfishness) ← false:
7. End for
8. While n_i(selfishness) ← true;
9. Call selfishisolate(n_i)
10. End While
11. End

3.3. Reconfirming the identification of Type I selfish nodes based on Enhanced Exponential Reliability Coefficient (EExRC)

The mobile nodes are recognized as Type I selfish nodes by utilizing Estimated Energy Metric which are examined through Enhanced Exponential Reliability

Coefficient (EExRC). This Exponential Reliability Coefficient is computed as follows.

Here the 'rp'is the number of packets received by the mobile node and 'fp' is defined as number of packets transmitted by that mobile node to its nearest node. Then, the packet drop (Dp) of the mobile node is computed according to the number of packets dropped by that mobile node, as given by (4)

Dp = rp -fp . (4)

The packet drop rate is computed for a mobile node is determined through (5)

DRp =Dpi/s. (5)

Through the value of packet drop rate, DRp the determined Exponential Failure Rate (ERF) by moving average scheme, which is calculated by (6)

$$ERF= \frac{\sum_{i=1}^{s} DR_{pi} \times P_i}{\sum_{i=1}^{s} P_i} \quad (6)$$

Where, P_i - priority factor

This priority factor (P_i) for each and every assembly 'i' is computed using (7),

Pi= (w(R_{req}) × Rreq + w(Rrep) × Rrep + w(Rerr) ×Rerr + w(DPt)×Dpt)+ D_{energy}+ AE2E Delay. **(7)**

Where, R_{req},R_{rep},R_{err}, D_{Pt} - normalized deviations factors of route request, route reply, route error and data packets respectively.

While, w(.)- weight allocated for every winning event of distributing route request acknowledgement packet , route reply acknowledgement packet , route error acknowledgement packet, data packet and malfunction event of distributing route request acknowledgement packet , route reply acknowledgement packet , route error acknowledgement packet and data packet.

$$R_{req}=\frac{R_{req-s}-R_{req-f}}{R_{req-s}+R_{req-f}} \quad (8)$$

$$R_{rep}=\frac{R_{rep-s}-R_{rep-f}}{R_{rep-s}+R_{rep-f}} \quad (9)$$

$$R_{err}=\frac{R_{err-s}-R_{err-f}}{R_{err-s}+R_{err-f}} \quad (10)$$

$$R_{pt}=\frac{D_{pt-s}-D_{pt-f}}{D_{pt-s}+D_{pt-f}} \quad (11)$$

Delay Model Based on Initial Energy of Nodes

A delay factor is computed according to the remaining power of nodes

$$D_{energy} = 1/(init* 100) . \quad (12)$$

Where,

D - delay

init - remaining energy of nodes

The delay is inversely proportional to residual energy; additional initial energy guides to lower delay. Here describe a predefined threshold value which is equal to 1 joule (for example) and place an initial energy of node to 10 joule. While residual energy is higher than threshold value, then the system gets lower delay else maximum i.e. 0.01 sec (for example).

Average End-to-End Delay (AE2E Delay)

This is the average delay among the transmitting data packet by the source and it's received at the matching receiver. This contains all the delays done during route acquisition, buffering and processing at neighbour nodes, retransmission delays, etc.

Then, the exponential reliability coefficient ExRC is manipulated using exponential distribution from ERF using (13)

$$ExRC = e^{-ERF.} \quad (13)$$

The ERCRM scheme predict a mobile node as Type I selfish node according to the value of Exponential Reliability Coefficient (ExRC). If the computed value of ExRC of a mobile node is predict to be lower than the exponential threshold value 0.40. Then the middle nodes are recognized as Type I selfish nodes.

Algorithm 2: (Priority Factor (Pi))

1. For every mobile node n_i in the Network N,
2. For each session i, i ∈ {1, . . . , s}
3. Calculate R_{req}
4. Calculate R_{rep}
5. Calculate R_{err}
6. Compute D_{pt}
7. Find the Priority Factor
8. End for (every session)
9. End for (every mobile node)
10. End.

Algorithm 3: (Enhnaced Exponential Reliability Coefficient)

1. For every mobile node n_i in Network N,

2. For each session j, j $\in$ (1, . . . , s)
3. Discover the number of packets fall by the mobile node through Dp(ni)$\leftarrow$ Difference (r_p; fp)
if$n_i \in$ Routingpath(S, n_1, . . . , n_m,d)
Otherwise Dp(n_i) $\leftarrow$0
4. Compute the packet drop rate of the mobile node ni as DRp(n_i) = D_{pi}/s
5. End For
6. Calculate the exponential failure rate as

$$ERF = \frac{\sum_{i=1}^{s} DR_{pi} \times P_i}{\sum_{i=1}^{s} P_i}$$

7. Calculate the exponential reliability coefficient through ExRC =e^{-ERF}
8. if (EExRC < 0:4 (threshold)
Allocate each node n_i(selfishness) $\leftarrow$true; otherwise
n_i (selfishness)$\leftarrow$ false:
9. End for
10. While n_i(selfishness) $\leftarrow$ true; do
11. Call selfishisolate (n_i)
12. End While
13. End

3.4 Isolation of selfish nodes from the routing path

It has been recognized that the execution of algorithm 3 in an ad hoc topology (Exponential Reliability Coefficient Computational algorithm) calculates Exponential Reliability Coefficient (ExRC) for every mobile node contributing in the routing activity based on second hand details such as packet drop rate and exponential failure rate attained from the neighbours. If the node has superior value of packet drop rate, then the exponential failure rate of the node gets increases, which in turn decreases the nodes' dependability factor. Hence, it is noticeable that the mobile nodes having lesser value of Exponential Reliability Coefficient have a better probability to exhibit type I selfishness behaviour.

Algorithm 4: Isolation of selfish nodes from the routing path

n – represents the mobile node
Algorithm (Selfish Isolation)
1. Initialization
2. For each routing path in the network
3. While n_i(selfishness) $\leftarrow$true do
4. Remove the node from the route
5. End While
6. find out a new routing path for transmission.
7. End for
8. End.

IV. EXPERIMENTAL RESULTS

In this section, the performance of the proposed Improved Exponential Reliability Coefficient based reputation Mechanism (IERCRM) is evaluated and compared with existing Exponential Reliability Coefficient based reputation Mechanism (ERCRM) scheme. The experiments are conducted using NS-2 simulator. The existing and proposed detection methods are compared in terms of end to end delay, throughput, and detection rate. The simulation settings are given in Table 1.

Table 1: simulationparameters

S.no	Parameters	values
1	Number of nodes	30
2	Selfish node	1 or 2
3	Dimension of simulated area	800 × 600
4	Routing Protocol	AODV
5	Transmission Range	250m
6	Packet size (bytes)	512
7	Simulation time (seconds)	100

Performance Evaluation

1. **End-to-end delay**

The average time taken by a packet to transmit from source to destination across the network is well-known as End to End delay

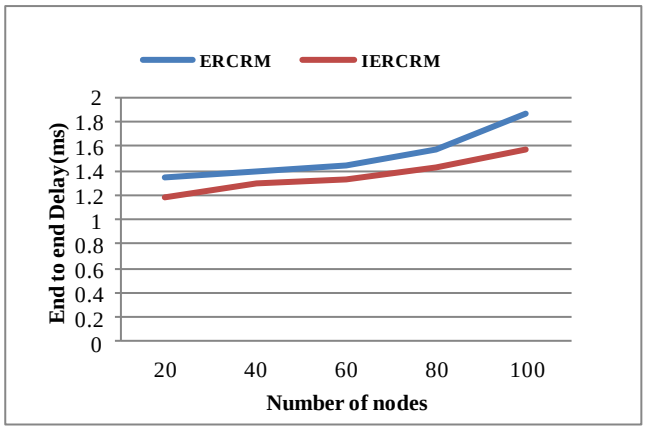

Figure.1. End-to-end delay comparison

Figure 1 shows the comparison of end to end delay performance for proposed Improved Exponential Reliability Coefficient based reputation Mechanism (IERCRM) and existing Exponential Reliability Coefficient based reputation Mechanism (ERCRM) scheme. The nodes are varying from 20 to 100 and end to end delay is plotted for such nodes in milliseconds (ms). From the graph it is clear that the Improved Exponential Reliability Coefficient based reputation Mechanism (IERCRM achieves less end to end delay.

2. **Throughput:**

The rate in which the data packets are successfully transmitted over the network or communication links is defined as throughput. It is measured in bits per second (bit/s or bps). It is also specified by units of information processed over a given time slot.

$$\text{Throughput} = \frac{\text{Number of delivered packet} * \text{packet size}}{\text{Total duration of simulation}} \quad (14)$$

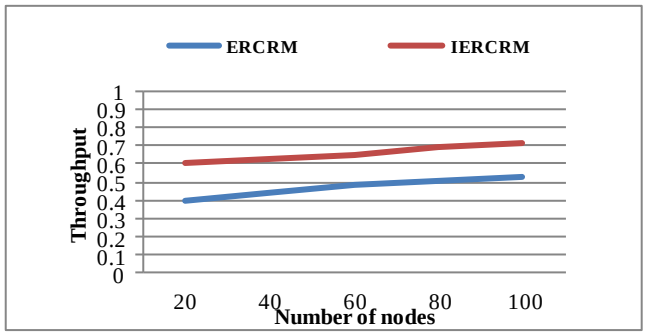

Figure 2.Throughput comparison

Figure 2 shows the comparison of throughput performance for Improved Exponential Reliability Coefficient based reputation Mechanism (IERCRM) existing Exponential Reliability Coefficient based reputation Mechanism (ERCRM) scheme. In X axis number of nodes are taken and in y axis throughput is taken. From the graph it is clear that the Improved Exponential Reliability Coefficient based reputation Mechanism (IERCRM) provides higher throughput than existing method.

3. **Detection rate:**

Detection rate is a factor which is used to determine the efficiency of the methodology to determine malicious node. It can be calculated by the following formulae,

Detection rate =(Number of true positive)/(Number of true positive + number of false negatives) (15)

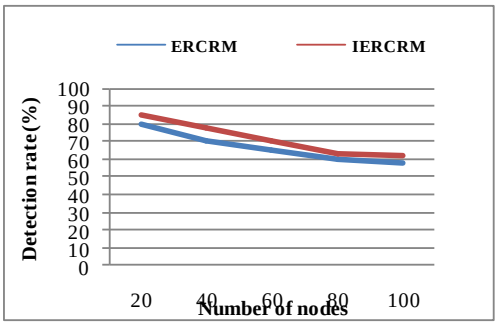

Figure.3. Detection rate comparison

Figure 3 shows the comparison of existing Exponential Reliability Coefficient based reputation Mechanism (IERCRM) and proposed Improved Exponential Reliability Coefficient based reputation Mechanism (IERCRM) in terms of detection rate. In X axis number of nodes are taken and in y axis detection rate is taken. It observe that, with the increase of network size (*i.e.*, increase of node number), the detection rates of both systems decrease, however, a notable decrease of selfish node detection scheme is observed.

V. CONCLUSION

The proposed system design an Improved Exponential Reliability Coefficient based Reputation Mechanism (IERCRM) for detection of selfish nodes from the routing path. The mobile nodes are predicted as Type I selfish nodes by using Estimated Energy Metric which are examined through Enhanced Exponential Reliability Coefficient (EExRC). In EExRC, the priority factor can be calculated based on packet routing , acknowledgement and delay based computation for ad hoc network. From the results the proposed IERCRM approach achieves better performance compared with the existing Exponential Reliability Coefficient based Reputation Mechanism in terms of performance evaluation metrics such as end to end delay, throughput and detection rate.

REFERENCES

[1] Hoang Lan Nguyen and UyenTrang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," IEEE ICNICONSMCL'06, 2006

[2] Yanchao Zhang , Wenjing Lou , Wei Liu, Yuguang Fang, " A secure incentive protocol for mobile ad hoc networks" in Journal of Wireless Networks , Volume 13 Issue 5, pp. 663-678 , October 2007.

[3] L. Buttyan and J.P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs", in Proc. of IEEE/ACM MobiHoc, Boston, Aug. 2000.

[4] L. Buttyan and J.P.Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," ACM Journal for Mobile Networks (MONET), Vol. 8, No. 5, Oct. 2003

[5] RubanaTarannum, YogadharPandey, "Detection and Deletion of Selfish MANET Nodes-A Distributed Approach" IEEE 2012

[6] Gagandeep, Aashima and Pawan Kumar. 2012. Analysis of different security attacks in MANETs on protocol stack. Int. J. Engg. Adv. Technol. 1(5): 269-275.

[7] P. Papadimitratos and Z.J. Haas, "Securing the Internet Routing Infrastructure", IEEE communications Magazine, 40(10), Oct, 2002.

[8] A. Babakhouya, Y. Challal, and A. Buouabdallah, "A simulation analysis of routing misbehavior in mobile ad hoc networks," in The Second International Conference on NextGeneration Mobile Applications, Services and Technologies NGMAST'08, 2008, pp. 592–597.

[9] Tan, WCW, Bose, SK & Cheng, TH 2012, 'Power and mobility aware routing in wireless ad hoc networks', IET communications, vol.6, no.11, pp.1425-1437.

[10] Michiardi P, Molva R. (2002). "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in International Conference on (CMS'02).

[11] Informant: Detecting Sybils Using Incen-tives N. Boris Margolin and Brian N. Levine Department of Computer Science, Univ. of Massachusetts, Amherst, MA, USA {margolin,brian}@cs.umass.edu.
[12]. Tarag Fahad & Robert Askwith"A Node Misbehaviour Detection Mechanism for Mobile Adhoc Networks " ISBN: I-9025-6013-9c 2006 PGNet
[13] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture," IEEE 2011.

Authors Profile

Mr. Daniel Nesa Kumar C pursed Bachelor of Science from Bharathiyar University, Coimbatore in 2006 and Master of Computer Applications from Bharathidasan University, Trichy in 2009 and Mater of Philosopy in Computer Science from Bharathiyar University, Coimbatore in 2013 and currently working as a Assistant Professor in Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore, Since 2009. He has published more than 15 research papers in reouted journals International journals and Conferences. His main research work focuses on Networking, DataMining, Image Processing. He has 9 years of teaching experience and 5 yrs of Research experience.

Dr. Saravanan V, pursed Bachelor of Science from Madurai Kamarajar University, Madurai in 1994 and Master of Computer Applications from Bharathidasan University, Trichy in 1999 and Mater of Philosopy in Computer Science from Manonmanium Sundaranar University , Tirunelveli in 2002 and Doctorate in Computer Science from Manonmanium Sundaranar University , Tirunelveli in 2016 and currently working as Professor and Head of the Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, Since 2004. He has published more than 35 research papers in reouted journals International journals and Conferences. His main research work focuses on Networking, DataMining, Image Processing, Cloud Computing, Big Data Analytics, . He has 19 years of teaching experience and 15 yrs of Research experience.

