A Novel Leader based Reputation Approach for Mobile Ad Hoc Networks

T. Sakthivel
Research Scholar,
Manonmaniam Sundaranar University, Thirunelveli,
Tamilnadu, India,
Pincode:627012

S. Vijaybhanu, PhD.
Assistant Professor
Department of CSE,
Annamalai University,
Chidambaram, Tamilnadu,
India, Pincode: 608002

RM.Chandrasekaran,PhD
. (Research Supervisor),
Professor, Department of CSE,
Annamalai University,
Chidambaram, Tamilnadu,
India,Pincode: 608002

ABSTRACT
Mobile ad hoc networks perform well only when nodes in the network cooperate in routing and packet forwarding. As these networks are lack of security aspects, selfish and malicious nodes become a part of that network resulting in performance degradation. This paper suggests a leader based reputation system for identifying routing misbehavior. The reputation system is constructed using trust value and decision made in routing that are based on past experience, observations and/ or informed behavior of other nodes. Trust value is evaluated using trust resilient algorithm and it is based on two important parameters namely, efficacy factor and feedback reliability. A node with high battery life and high trust value is elected as a leader. The member nodes report the reputation value and feedback to the leader. The leader node maintains a reputation and feedback records of all its member nodes. The reputation value is an integer value and feedback is just a phrase conveying the satisfaction level of performance of a node. A node with continuous negative feedback is treated as a malicious node and isolated from the network. Feedback is aggregated using modified periodic per hop adaptive aggregation techniques. This proposal detects a malicious node effectively and avoids false reporting as it considers only feedback from the highly reputed node. We perform an overall analysis of our paper by simulation using the network simulator (NS- 2). The experimental results clearly indicate the effectiveness and advantages of our proposed system in eliminating misbehaving nodes.

Keywords
DSR, MANETS, Node Cooperation, Node reputation, Trust Evaluation, Leader Election, Node misbehavior

1. INTRODUCTION
1.1 Ad hoc networks

A Mobile Ad hoc NETwork(MANET) [1] is more vulnerable to routing attacks due to its open nature of medium, decentralized administration, lack of security, dynamic network topology, multi- hop routing, energy limited operation, lack of scalability etc. There are high probabilities for misbehaving node to launch any kind of attack in MANETs. The misbehaving nodes are of two kinds namely selfish and malicious. Selfish nodes use the network resources only for their own purposes and do not participate or cooperate in the routing process. Unlike selfish nodes, malicious nodes do not conserve battery life but they indulge in wasting the network resources. Due to their greater vulnerability, MANET should consider the security system as a mandatory to protect its user from routing attacks despite of the application environment. Security concepts alone do not guarantee integrity of MANETs but it should be accompanied by node's cooperation in the routing process. The routing protocol used in our paper is DSR[2]. This work adds reputation mechanism to the existing DSR protocol to mitigate the malicious and selfish activity of nodes during the routing process. Each node store route caches that include the route it knows. Whenever a node finds a new route, the node updates it in its cache. This mechanism is used to update reputation values.

1.2 Misbehaving nodes in Adhoc networks

Now- a- days, MANET is tremendously used in the communication world. It makes use of all nodes in the network for broadcasting and routing. Among the nodes in the network, a node may misbehave by promising to forward packet to other nodes but it fails to do so. Misbehaving nodes may be classified as selfish, malicious and inactive [3]. A selfish node hesitates to forward the packet in order to maintain its battery life or it is not willing to waste the available network resources. A malicious node drops the packets and thus results in denial of service. There is some dangerous kind of misbehavior that they cannot be detected easily and devastating the network performance. This kind of misbehavior can only be solved by reputation systems. The main function of a reputation system is to monitor and rate the behavior of nodes in the network. This rating is performed at the routing and forwarding phase so that the nodes can report according to their own opinion about the nodes they know. The belief of one node is estimated by another node is called reputation. The main aim of the reputation system is to distribute the ratings of all nodes in the network so that they will be aware of malicious nodes. The reputation helps in determining the number of cooperating and non cooperating nodes in the network. The reputation system can be used to detect any kind of misbehavior in the network.

1.3 Reputation systems

Reputation system [4] is the concept commonly used in on-line transactions. The term reputation is used to represent the observed quality ratings of a node by others. In MANETs, it means the performance level of a node in the routing process. On the other hand, the term trust represents the honest level of a node in the supporting protocol that intends to protect base protocol. In the MANETs, reputation system is mainly used to detect misbehaving nodes. Reputation systems gather information only based on observation that facilitates a node to detect misbehaving nodes and mitigate its harmful effects [5]. A node may not interact with all nodes in its multi-hop

paths instead; all other nodes are advertised about the decision of routing path. There are various forms of reputation based on the type of observation. The most commonly used reputation systems are subjective reputation, indirect reputation and functional reputation [6]. The reputation computed from direct observation made by a subject is referred as subjective reputation.

1.4 Aim and objectives

To design an effective leader based reputation system that mitigates the effect of misbehaving nodes.

To encourage the trusted nodes, it acts in the same manner and to discourage non- trusted nodes from the participation in the routing process.

To elect a node as a group leader node that maintains reputation value and feedback of all nodes under its control.

The leader node provides service to the nodes that has high reputation value and thus preventing false reporting.

1.5 Leadership concept

The reputation value is now calculated and stored in the packet header. Our proposed work implementation is based on DSR protocol. In a group of network, a leader node is selected on the basis of some criteria such as high connectivity, high battery life etc. The leader node maintains a record of reputation value of all other nodes under its control. Whenever the reputation value changes locally, the leader node updates its reputation record based on tracer observation. The leader node takes the role of central authority of the network. The member node requests the leader node for feedback about a node to which it is going to communicate. The leader node maintains both reputation record and feedback record. When a node requests a service to the other node, it posts feedback to the leader node whether that node provided the requested service or not. The leader node accepts the feedback only if the reputation value of the corresponding node is higher. When the node gets repeated negative (low) feedback, it is treated as a malicious node. The leader node maintains the list of malicious nodes. This concept makes our proposal effective in detection of malevolent nodes.

1.6 Paper organization

The paper is organized as follows: section 2 explains the related work. Section 3 provides a brief overview and introduction about the proposed system. Section 4 proposes an effective leader based reputation mechanism for the detection of misbehavior. Section 5 provides simulated results. Section 6 concludes this paper.

2. RELATED WORKS

The watchdog method is used to detect the misbehaving nodes in the MANETSs [7]. Consider a situation in which the source node, S sends the packet to the destination node D only through intermediate nodes X, Y and Z. The intermediate node Y attempts to forward the packet to D from S through Z. On transmission, X can overhear the transmission of Y and come to a conclusion that Y has forwarded the packet to the next intermediate node. The Pathrater is executed by all the nodes in the network and it creates the awareness of the misbehaving node in the network. Every node maintains a record of rating for other nodes within its transmission range of the network. A path metric is estimated by considering the net average of node ratings in the routing path. The path metric is chosen as it provides a comparative analysis of the general reliability of various paths and if there is no reliable path, then the pathrater design a shortest length path algorithm. A destination node may have several paths but the shortest path is selected which has a highest metric. The difference between the pathrater and the basic DSR is that the DSR selects the shortest path in the route cache but the pathrater selects the path which has the highest path metric in the routing path [7].

Another effective method for detecting misbehaving node is CONFIDANT [8]. Reputation and trust value is calculated based on the observation and experience about behavior of other nodes. It is based on DSR protocol and it is deployed at the top of DSR. A factor of re-socialization and re-integration has been introduced. The CONFIDANT comprises of four major components such as a monitor, reputation system, trust manager and path manager. The monitor component deploys "neighborhood watch" in which deviating nodes are observed locally. The trust manager component deals with ALARM messages to warn the other nodes about the misbehaving nodes. After a node has gained information about malicious nodes, it passes ALARM messages to a group of nodes.

CORE insists on the co-operation of nodes in MANETs [9]. It is mainly designed to prevent selfish misbehavior of a node. In CORE, the reputation value is calculated depending on the collaboration rate of the nodes. CORE is a generic technique that is compatible with the existing routing protocols. The CORE system makes use of network entity, a reputation table and watchdog mechanism. The CORE concept is then applied to DSR, and packet forwarding method. The reputation table must be updated according to the positive ratings of the cooperating nodes.

The nodes in the MANET takes decision according to the information gathered by its own and from their neighbors [10]. The information spreaded may be good or bad and this has a greater impact on the reputation system deployed. The effect of rumors and robustness of the reputation system is investigated with respect to detection time and false accusations respectively. A Bayesian technique is proposed mainly for representation and updates of the reputation system. Liars are detected and isolated from the network. The Bayesian system is much effective in providing robustness against improper accusations. Even, the second hand information can considerably improve the detection mechanism and can be extended for isolation of malicious nodes. Fake observations may mislead nodes and the robustness of the reputation system may get decreased.

One of the major issues in MANET is computation complexity. Since it is distributed in nature, it is divided into a number of cluster. Each cluster has exactly one leader and is elected on the basis of cluster based protocol [11]. In the first stage, the protocol deploys an algorithm for cluster formation and then, a cluster head is elected. In the second stage, the leaders of each cluster are connected by an algorithm called ring formation. In the final stage, a super leader is selected among these cluster heads using Chang Roberts's algorithm. This kind of cluster formation considerably reduces the computational cost and it is a scalable method.

The application of leader election is extended to the intrusion detection system. The node with more energy resources is elected as a leader node. The leader is selected in the network

that has selfish nodes. To preserve its energy, a node may lie about its own resources. A mechanism based solution is provided to overcome the selfish node issues. Reputation based incentives are provided to the nodes to truthfully take part in the process of leader selection. To reduce the election overhead, some of the election algorithms are deployed at reduced cost. This proposal is applied in two scenarios: cluster dependent and cluster independent. Leaders are elected in both these scenarios [12].

3. PROPOSAL OVERVIEW

The main processes in the reputation system are representation, construction and update of reputation. The reputation is an opinion of a node. The reputation and trust are closely related and together they form an effective reputation system [13]. The nodes do not take the decision only by its own experience but also share information from its neighbors. The components in a reputation system are tracer, reputation and reaction. Each node contains these components for the detection of misbehaving nodes. Our reputation system is based on direct or subjective observation. Tracer is used to observe the activities or behaviors of other nodes in the network. Based on the observation made, feedback reliability and efficacy factor are calculated. Finally, the trust value is estimated using trust resilient algorithm. If the trust value of that particular value does not exceed the threshold value, then it is a malevolent node.

There are numerous routing and forwarding attacks in MANETs. Our paper aims to design a novel reputation system that detects the following malignant activities of a malicious node. Some of the malignant activities are as follows:

* Do not forward any of the control messages or data packets

* Try to gain all network traffic towards it by a fake advertising

* Purposely re- route the traffic link even though there is no route error has been occurred.

* Do not forward the error message though an error message has been observed.

* Route updates may be performed unnecessarily.

* Silent interference in the routing process i.e. message header of data packets or control messages may be tampered.

Some of the basic assumptions made in our reputation system are: The nodes keep on interacting with all other nodes in the range within which it can communicate. In a group of nodes, all of them must be capable of tracing the activities of all other nodes and must be able to evaluate trust. Each node should maintain a trust table for storing the trust level of other nodes in its group. This kind of reputation system is required to solve the security issues in MANETs as mentioned in [14].

The traced information is reported to the reputation component in the form of feedback. Feedback is just a phrase that expresses the satisfaction level of its neighbor's performance like packet forwarding. The trust evaluator evaluates the faith level of other nodes that it cares about in the network. To make our proposal effective, a group leader node is selected and it is responsible for maintaining entire reputation value. A leader node is selected on the basis of high connectivity, high battery power and high reputation value [15]. Whenever, there is a communication between two nodes, the service requestor must report feedback about the service provider to the leader node. The leader node must accept the feedback only if the feedback source has high reputation value. The leadership concept is introduced in the reputation system to detect the malevolent nodes effectively and to prevent false reporting. A leader node takes a final decision whether a node must continue routing or must be isolated. If a node gets negative feedback continuously, it is marked as malicious nodes and isolated from the network. The leader maintains a list of malicious nodes. The leader node may fail which leads to a single point of failure. In case of leader failure, a new leader is elected as a leader and current trust values are assigned to the new leader.

4. LEADRE BASED REPUTATION SYSTEM

The reputation system is considered as the only effective approach for the detection of more than one routing attacks on the MANETS. Each node is deployed with the reputation system and this reputation system has three components namely tracer, reputation component and reaction component.

4.1 Tracer

The goal of the tracer is to collect the direct observation about the behavior of nodes in MANET. The abnormal behavior of a node can be distinguished from a normal one using tracer through direct observation [16]. Not packet forwarding alone considered as misbehavior but it includes some dangerous routing attacks like wormhole attack, black hole attack, grayhole attack etc. Most of these attacks can be detected by the reputation system using direct observation. A node can trace the activities of nodes within its communication range. The nodes in the reputation system can distinguish abnormal activities from the normal node activities by observing to the transmission of the neighboring node. Being one of the components in the reputation system, the tracer, traces all these abnormal activities of nodes. It is then reported to the reputation component in the form of feedback. It reports the feedback to the leader node about its neighbor's performance in the routing process. Feedback is a phrase i.e. a node commenting on its neighbor's activities in the routing process. The reputation component works with the information reported by the tracer. Using the tracer, a node collects information about other nodes in passive mode. The required information about the activities of other nodes can be gathered by analyzing sent and received packets. The possible information that can be collected from a node is sent and received data packets, sent and received control packets, and number of received frames. This information is directly or indirectly related to the trust and reputation values.

4.2 Trust parameters

On the basis of information traced, each node calculates the trust parameters such as feedback reliability and efficacy factor. These are vital parameters to calculate trust of each node.

4.2.1 Efficacy factor

It is a measure of involvement of a node in the routing process. This parameter is equally important to feedback reliability parameter for trust estimation. If a node actively participates in the packet forwarding process then its efficacy factor will be high and its value ranges from 0.1 to 1. The value of efficacy factor can be determined in two ways. One is

to estimate the total number of packets sent and received successfully. Secondly, a node's CPU and memory utilization, battery level can also be measured quantitatively to estimate the involvement of a node in the routing and packet forwarding process. A simple mathematical expression for efficacy factor E(A) is given in equation (1).

$$E(A) = \sum (Tr(x) + Rr(x)) - \eta \qquad (1)$$

Tr (x) and Rr (x) denotes the transmitted and received packets successfully in a certain period and η is the effectiveness of the transmitting node. This is an important parameter to calculate trust and it can identify the selfish nodes easily. If the total number of packets sent and received is less, it is considered as a selfish node.

4.2.2 Feedback reliability

During the interaction between two nodes A and B, they provide feedback about each other based on their performance at routing. The feedback is just a phrase of various length expressing A's service satisfaction level on B and vice versa. Some of the nodes may provide fake feedback about another node intentionally. Therefore, a genuine node may be given fake feedback and isolated from the network by malicious nodes, though it performs well in the routing process. In our paper, we consider the feedback reliability parameter to calculate the trust values in addition to the efficacy factor. The nodes with higher feedback reliability are awarded higher trust value than that of lower feedback reliability.

The feedback reliability can be estimated on the basis of history of the node's behavior that posts feedback. The feedback reliability of node A is estimated through other node's interaction with node A. The other nodes in a group provide feedback about node A to leader node. The leader node decides the level of feedback reliability. Some nodes may post positive feedback on node A and others may post negative feedback. The feedback from highly trusted nodes is considered for computing feedback reliability. Then the leader node checks the matching level between feedback on the node A by other (neighboring) nodes. If there are more deviations in the matching level, then the feedback reliability is low.

4.3 Reputation component

An effective reputation component should meet the following two requirements. The first requirement is that it should provide incentives for well behaving nodes to prevent negative effects of a bad reputation system. The second one is that, it provides a list of trusted nodes and trusted routes for the entire network system [17]. The estimation of trust value is based on the trust parameters that discussed in the section 4.2.

4.3.1 Trust evaluator

Trust is a faith level of a node that is determined based on its action at the routing and packet forwarding process. The trust level shows to which extent one node trusts another node based on its behavior. Trusted nodes obey the protocol order and acts accordingly. The trust evaluator evaluates the trust on observed information from the tracer for a particular event. A node can collect information about another node either directly or indirectly from other nodes for a specific event. Since the MANETs are dynamic in nature, the evaluation of trust in a discrete manner is not suitable. Though, discrete trust values are simple to represent and categorize the trust level, is not suitable for trust evaluation in the MANET as nodes in the network have greater mobility. In the MANET, the time period taken for local observation and interaction are too short and so the trust must be represented as a continuous range of values that will be easy for differentiation of various levels of trust values.

Trust evaluation involves in the allotment of efficacy factor and feedback reliability to the happenings traced by the tracer. The trust evaluator starts the evaluation soon after it receives the reports from tracer. The allotment of efficacy factor relies on the type of application to which trust is evaluated and it is a time variant function. Each node assigns efficacy factor in a dynamic manner based on its own principles and circumstances. The negative trust evaluation is encouraged in our approach as it is convenient for the reputation system to isolate the malicious nodes. The average trust values for a node's activity by another node are then calculated by combining individual efficacy factor. Let us define the trust (T) of node A as T (A) and it can be expressed as:

$$T(A) = \sum_{J=1}^{n} \{E_A(j) * C_A(j)\} + R_e(N(A,n)) \qquad (2)$$

E_A (j) and C_A (j) in equation (2) indicates the efficacy factor of j^{th} traced event of node A and the circumstantial trust of node A in the j^{th} event traced by the tracer. Each node in a group maintains the trust value of other nodes with which it has communicated recently in its cache and represented as trace cache. A node must go for trust computation of another node only when it does not contain that node's trust value in the cache. Instead of recursively calculating the trust value, it is sufficient for a node to retrieve the recently computed trust values that are stored in the cache. Reliability of neighbor node's feedback on node A is denoted as Re (N (A, n)). This technique reduces the computational overhead. A trust resilient algorithm for trust calculation is given.

Algorithm 1: Trust Resilient Algorithm

Retrieve feedback from the leader node

For (1<j<maximum feedback length) do

N (A, n)← nodes with reliable feedback

If tr.cache ≠ empty, then

Re (N (A, n))← tr.cache (N (A, n))

Else

Compute trust value using equation (2)

End if

End for

tr.cache (A)← T (A)

If

T (A) > Threshold

Mark it as genuine node

End if

Post the trust value of node A, T (A) to leader node

4.4 Reaction component- Leader node and its functions

The reaction component encourages the node with high reputation value to actively participate in the routing process and discourages the nodes with negative reputation value [18]. The reaction component includes the leadership mechanism. Since, the reputation system is our main focus, the selection and renewal of a new leader is not given much importance in our paper. In a cooperative network, there is a group leader that has some sort of additional responsibilities in achieving an effective network without malicious nodes. In our proposed work, a node is chosen as a group leader and it acts like a centralized authority. Each node calculates the reputation value of other nodes and reports it to the group leader node. A leader node has some additional responsibilities than other nodes. For a node to be a leader, it must meet the following requirements:

* A node must remain in a network for a long period with high connectivity.
* A node must have higher trust value.
* A node must actively participate in the routing process with high battery life.

A node with all the above mentioned features can be chosen as a leader. It maintains a record of reputation value of all other nodes under its leadership. A leader node collects information from other nodes and maintains as a record. Whenever, a node is in need of feedback of the other node, it should make a request to the leader. The leader node sends back feedback reply only if the reputation value of that node is higher than the threshold value.

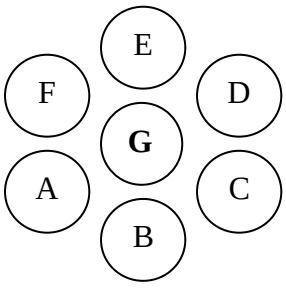

Fig 1: A group of nodes with their group leader

Consider the Fig 1 in which a group of nodes (A, B, C, D, E, F, G) with their group leader G. The node B requests a service to node C after B checking the reputation value of C. After C provides service, B reports the feedback about node C to the group leader, G. The node G accepts the feedback only if the B's reputation value is high. Whenever a node request a service to neighbors and gets a service, it must report to the group leader. The group leader then aggregates this feedback and provides services to other nodes by referring to aggregated feedback. Suppose if the node D wants to know about node C, it may make a request to G for feedback about node C. Consequently, the node G refers to the aggregated feedback and then responds to D's request only if the reputation value of D is high. The nodes A, B, C, D, E and F posts their feedback to G about their satisfaction level regarding neighbor node's performance in the routing process. This scheme prevents the false reporting effectively.

Functions of a leader node

* Gathers each node's experience in routing and feedback about its neighbors.
* Maintains a record of reputation value of nodes under its leadership.
* Accumulation of feedback of each node by its corresponding neighbors.
* Responds to feedback request by a node by referring to the reputation record.
* Must checks the reputation value of a node before sending feedback response.
* Maintains a list of malicious nodes.

4.5 Feedback aggregation

In our paper, we have considered modified periodic per hop adaptive aggregation technique. In periodic per hop adaptive aggregation technique, it adjusts the node's timeout period based on the position of a node in the MANETs [19]. In the modified periodic per hop adaptive aggregation technique, a leader node collects feedback from its member nodes and stores in its cache. Feedback aggregation is carried out when a leader node receives feedback from its member node after a certain period of time. In the periodic per hop adaptive aggregation technique, partial aggregation is carried out in which intermediate nodes perform feedback aggregation. But, in the modified periodic per hop adaptive aggregation technique, direct aggregation is introduced in which only a leader node performs feedback aggregation. Periodic aggregation is suggested as it reduces aggregation overhead. A group leader aggregates the feedback of one node from other nodes in two categories namely, "High" and "Low". The nodes with positive feedback are aggregated in a "High" category. The nodes with negative feedback are aggregated in a "Low" category. A group leader must consider a feedback only if it is given by a node with high reputation value. Feedback from the nodes with high reputation value are considered to be true and are given first preference. When a node, request or enquire for a feedback about of another node, the group leader node must check for the requester reputation value. If the requestor's reputation value is high, then the group leader responds to its request otherwise the group leader ignores the request. Whenever an event takes place locally i.e. a route request or reply is accepted or rejected, these local feedback is updated by the leader node. The feedback is updated in a periodic manner and if there is no change in the local feedback mechanism for a particular time, a leader's feedback system remains same.

4.6 Malicious node detection

When a communication between two nodes takes place for the first time, the report is sent and added to the leader's feedback system. When there is a change in the tracer observation locally, the reputation value maintained by the leader node also changes. When a node gets negative (low) feedback repeatedly, it is marked as malicious nodes and isolated from the network. The leader maintains a list of malicious nodes. The member nodes should check the malicious node list in the leader node before communicating with any other nodes. The

effectiveness of the reputation system can be calculated with the increased network throughput and the reduced number of dropped packets. A leader node aggregates the feedback from its member node only if it has high reputation value. Therefore, the probability of false reporting is much reduced. If the trust value exceeds the threshold value, then it is a genuine node. There are threshold determining factors like eagerness to trust other nodes, adaptability of a node with the successful transaction at any situation, etc. In our paper, an optimal threshold value is chosen on the basis of service history of a node. A leader node contains a list of malicious nodes for future reference and it is much helpful for newly entering nodes.

4.7 Block diagram

The block diagram of the proposed reputation system is shown in the Fig 2. It briefly explains the functions of components of the reputation system.

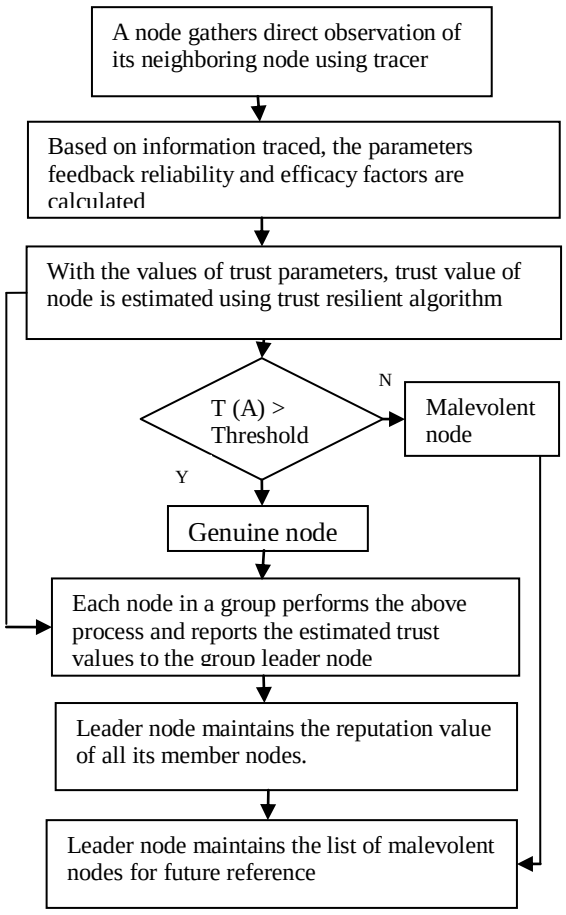

Fig 2: Block diagram of the proposed reputation system

5. PERFORMANCE EVALUATION

5.1 Simulation set up

The performance is evaluated using NS2 network simulator with CMU wireless extension [20]. The leader based reputation is the add-on to DSR protocol. 200 mobile nodes each with communication range of 200m were randomly distributed in a 900m X 900m flat area. IEEE 802.11 is used in MAC layer with a channel rate of 11mbps. Speed of the node varies from 0-20 m/s. Mobility scenario is based on random way point model with Constant Bit Rate(CBR) traffic. The packet size is 128 bytes. Total simulation time is 1000s. The nodes are selected randomly as the sender, the receiver and the malicious nodes. The experiment is repeated for 6 times.

5.2 Performance metrics

5.2.1 Throughput

It is the ratio of the total number of packets forwarded to that of packets received by the specified destination.

5.2.2 Efficacy factor

The efficacy factor of a node is defined as how well the node utilizes the network resources for packet forwarding. It indirectly represents the involvement of a node in the routing and packet forwarding. This includes the amount of power consumption, CPU and memory utilization. The efficacy factor of a node can be defined as:

E= (a sum of the benefits of sent and received packets) –

(effectiveness of the packet transmitting node) (3)

5.2.3 Routing overhead

Routing overhead is the ratio between transmissions of the routing process (RREQ, RREP, RERR and tracing) and simulated data transmission. Overhead is related to the number of transmissions during routing. The transmission of control packets is more expensive than data packets. The mathematical representation of routing overhead (O_R) is given in the equation (4).

$$O_R = \frac{1}{\sum (RREQ + RREP + RERR) \text{ /for each transmission/}} \quad (4)$$

5.2.4 Packet delivery ratio

It is the ratio of packets sent or forwarded by the sender and number of packets that are received by destination successfully among the transmitted packets.

5.3 Performance analysis

5.3.1 Throughput

The throughput of the proposed reputation system is shown in the Fig 3. The graph has been plotted for the number of malicious nodes Vs throughput. The throughput is calculated as the number of data packets sent or forwarded that is received by intermediate nodes or destination versus the number of malicious nodes. In Fig 3, throughput of the proposed system and CONFIDANT is compared in which both the mechanisms achieve 97% of throughput when the network contains no malicious nodes. In the presence of malicious nodes, the throughput decreases gradually but there is a difference between the throughput level of the proposed system and CONFIDANT. When the number of malicious nodes is 50, throughput of the proposed system is 33% while that of CONFIDANT is only 9%. This mechanism increases throughput up to 25% when compared to the existing CONFIDANT protocol.

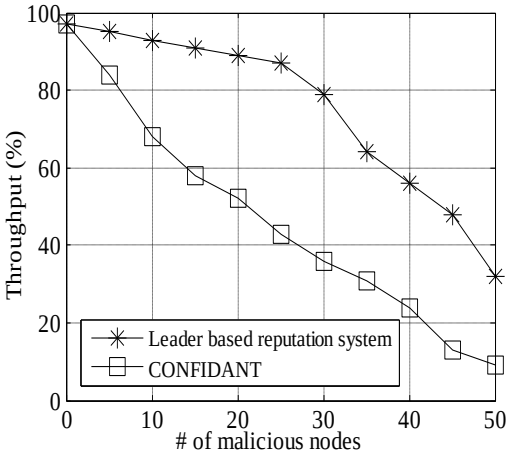

Fig 3: Throughput comparison

5.3.2 Routing overhead

The effect of routing overhead in the proposed system is shown in the Fig 4. The routing overhead is a little bit high in the proposed system as it sends many control messages towards destination only through the known routes that comprise of malicious nodes in it. Any control message generated by it may flood the network that significantly increases the overhead. As the reputation systems involve direct and local observation on each node's activities, the overhead will be high. The calculation of reputation value also increases the computational overhead but compensates in terms of throughput and packet delivery ratio in the presence of malicious nodes.

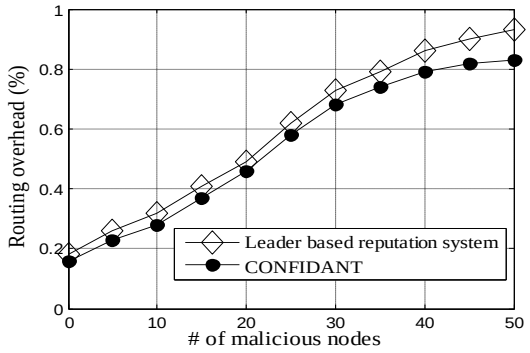

Fig 4: Routing overhead Vs percentage of malicious nodes

5.3.3 Efficacy factor

The efficacy factor versus no of malicious nodes is shown in the Fig 5. This factor indicates the level of network utilization of a node for participating in routing and packet forwarding. This factor is then calculated for all nodes in the network by averaging the individual efficacy factor. This factor is related to the number of transmissions by the sender and response from the intermediate nodes. Both the systems have a highest efficacy factor in the absence of malicious nodes. The proposed reputation system maintains good efficacy factor until it detects 50 percentage of malicious nodes and then, efficacy factor reduces gradually. In the absence of the reputation system, the overall efficacy factor in the network decreases rapidly.

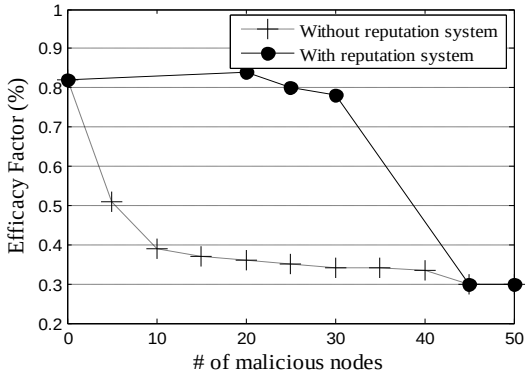

Fig 5: Efficacy factor Vs percentage of malicious nodes

5.3.4 Packet delivery ratio

The comparison of the packet delivery ratio with the proposed reputation system and without reputation system is shown in Fig 6. This parameter plays a significant role in the estimation of the performance level of the proposed system. As the proposed reputation system detects the malicious nodes in an effective manner its packet delivery ratio is greater when compared to other mechanism or without any reputation system. The packet delivery ratio of the system without the reputation system decreases constantly. The proposed reputation system maintains a constant packet delivery ratio to some percentage of malicious node. As the percentage of the malicious nodes increases, the packet delivery ratio decreases gradually. The packet delivery ratio and the percentage of malicious nodes are indirectly proportional to each other.

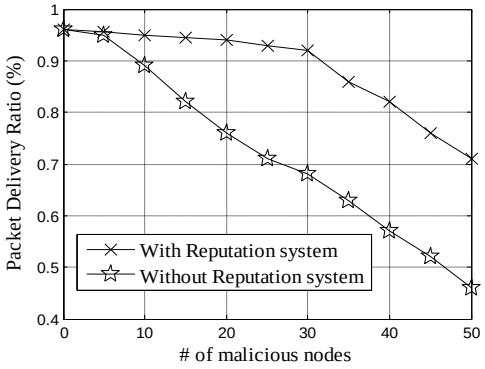

Fig 6: Comparison of packet delivery ratio

6. CONCLUSION

MANETs have several security issues due to its dynamic nature. Therefore, it is much vulnerable to several kinds of routing attacks. A novel reputation system is proposed that is used to establish trust level between nodes and enforce trustworthiness among nodes. Two effective trust parameters i.e. feedback reliability and efficacy factor are considered to calculate trust using trust resilient algorithm. Simulation results, make it clear that, the proposed reputation system is much effective in the detection of malicious nodes. In our proposed system, the node's activities are traced and reputation value is calculated using reputation component.

Finally, the reputation system responds to the estimated reputation value using reaction component based on leader node. A leader node takes the role of central authority (in wired networks) and overcomes some of the wireless network issues. A node with continuous or repeated negative feedback is isolated from the network. Leader node maintains the list of malicious node. The leadership concept in reputation system makes our proposal effective in detecting malevolent nodes and in avoiding false reporting. Trust resilient algorithm acts as an effective defense mechanism for all kinds of routing attacks and the correctness of the proposed system has been verified using network simulator (NS- 2).

7. REFERENCES

[1] Imrich Chlamtac, Marco Conti, and Jennifer J. N. Liu "Mobile ad hoc networking: imperatives and challenges" Elsevier transactions on ad hoc networks, volume 1, pp. 13- 64, 2003

[2] David B. Johnson and David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", in Mobile Computing, pp. 153-181, Kluwer Academic Publishers, 1996.

[3] Matthias Hollick, Jens Schmitt, Christian Seipl, and Ralf Steinmetz "On the Effect of Node Misbehavior in Ad Hoc Networks" IEEE international conference on communications, volume 6, pp. 3759- 3763, 2004

[4] Paul Resnick, Richard Zeckhauser, Eric Friedman, and Ko Kuwabara "Reputation Systems: Facilitating Trust in Internet Interactions" communications of ACM, volume 43, issue 12, 2000.

[5] Kun Zeng, Przemysław Pawelczak, and Danijela Cabric "Reputation-Based Cooperative Spectrum Sensing with Trusted Nodes Assistance" IEEE communications letters, volume 14, issue 3, 2010

[6] Po-Wah Yau and Chris J. Mitchell "Reputation Methods for Routing Security for Mobile Ad Hoc Networks" IEEE transaction on mobile future and symposium on trends in communications, pp. 130- 137, 2003

[7] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" ACM proceedings of the 6th annual international conference on mobile computing and networking, pp. 255- 265, 2000.

[8] Sonja Buchegger and Jean Yves Le Boudec "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Adhoc NeTworks)" proceedings of 3rd ACM international symposium on mobile Adhoc networking and computing, pp. 226- 236, 2002

[9] Pietro Michiardi and Refik Molva "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks" Springer transaction on advanced communication and multimedia security, pp. 107- 121, 2002

[10] Sonja Buchegger and Jean-Yves Le Boudec "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks" WiOpt'03 proceedings on modeling and optimization in mobile, ad hoc and wireless networks, volume 1, 2003

[11]Orhan Dagdeviren and Kayhan Erciyes "A Hierarchical Leader Election Protocol for Mobile Ad hoc Networks" LNCS, volume- 5101, pp. 509- 518, Springer, 2008

[12] Noman Mohammed, Hadi Otrok, Lingyu Wang, Mourad Debbabi and Prabir Bhattachary "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET" IEEE transaction on dependable and secure computing, volume 8, issue 1, pp. 89- 103, 2011

[13]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, pp. 37- 42, 2005

[14] Lidong Zhou and Zygmunt J. Haas "Securing Ad Hoc Networks" IEEE transaction on network, volume 13, issue 6, pp. 24- 30, 1999

[15] Sudarshan Vasudevan, Brian DeCleene, Jim Kurose, and Don Towsley "Secure Leader Election in Wireless Ad Hoc Networks" IEEE proceedings of DARPA information survivability conference and exposition, volume 1, pp. 261- 272, 2003

[16] Jochen Mundinger and Jean-Yves Le Boudec "Analysis of a Reputation System for Mobile Ad-Hoc Networks with Liars" Elsevier transaction on performance evaluation, volume 65, issue 3- 4, pp. 212- 226, 2008

[17] Sonja Buchegger and Jean-Yves Le Boudec "A Robust Reputation System for Mobile Ad-hoc Networks" EPFL IC Technical report IC/ 2003/ 50, 2003

[18] Mohamed Tamer Refaei, Luiz A. DaSilva, Mohamed Eltoweissy, and Tamer Nadeem "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks" IEEE Transactions on computers, volume 59, issue 5, 2010

[19] Elena Fasolo, Michele Rossi, Jorg Widmer and Michele Zorzi "In-network Aggregation Techniques for Wireless Sensor Networks: A Survey" IEEE transactions on wireless communications, volume 14, issue 2, pp. 70- 87, 2007

[20] "The Network Simulator (ns-2)," http://www.isi.edu/nsnam/ns/, 2012

8. AUTHOR PROFILE

T. Sakthivel has received B.E. (Computer Science and Engg.) from University of Madras in 1995, M.Tech. (Information Technology) from Punjabi University in 2003, currently pursuing Ph.D. from Manonmaniam Sundaranar University, Thirunelveli, Tamilnadu, India. He has more than 12 years of experience in teaching and industry. His research interest includes Networks, Wireless Ad Hoc Networks and Network Security.

Dr. S. Vijay Bhanu is currently working as an Assistant Professor, Department of Computer Science & Engineering, Annamalai University, Chidambaram, Tamilnadu, India. He has received Ph.D from Anna University, Coimbatore in 2012. He served as wing Head, DDE, Annamalai University, Chidambaram for nearly five years. He served as Additional Controller of Examination at Bharathiar University, Coimbatore for two years. He conducted a workshop on Business intelligence in the year 2004. He has published three papers in international journals. He is a life Member in Indian

Society for Technical Education. His research interest includes Wireless Networks and Software Engineering.

Dr.RM.Chandrasekaran is a Professor at the Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Tamilnadu, India. He served as a Registrar of Anna University, Tiruchirappalli from 2007 to 2010. From 1999 to 2001 has worked as a software consultant in Etiam, Inc, California, USA. He received his Ph.D degree in 2006 from Annamalai University, Chidambaram. He has conducted workshops and conferences in the area of Multimedia, Business Intelligence, Analysis of Algorithms and Data Mining. He has produced four Ph.Ds. He has presented and published more than 40 papers in conferences and journals and is the co-author of the book Numerical Methods with C++ Programming(PHI,2005). His research interests include Data Mining, Algorithms and Mobile Computing. He is a life member of the Computer Society of India, Indian Society for Technical Education, Institute of Engineers and Indian Science Congress Association.