Received: June 25, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Reliable Trustworthy Approach Based on Node Behavior Prediction for Secure Routing in MANET

Kotari Sridevi[1]*   **Mandapati Sridhar[2]**

[1]*Acharya Nagarjuna University, Nagarjuna Nagar, Guntur, Andhra Pradesh, India*
[2]*Department of Computer Applications, R.V.R &J.C College of Engineering,*
Guntur, Andhra Pradesh, India
* Corresponding author's Email: devijak@gmail.com

Abstract: An unstructured version of a traditional wireless network provides a mobile ad hoc network (MANET) that is well suited for emergencies. However, due to lack of infrastructure and resource limitations, many performance problems occur at the same time. High-security vulnerabilities are likely to arise, largely because of dynamic behavior, and the complete communication cycle dependent on unidentified nodes which join and leaves as they want. Several past security schemes studies suggested that reliable and trusted nodes can minimize communication overhead and achieve higher throughput. This kind of scheme affects the route chosen for communication because it cannot distinguish between intentional and unintentional errors at runtime. It is, therefore, important to categorize node activities and also provide a node recovery scheme to regain their original reliability for the genuine nodes. In this paper, we propose a Reliable Trustworthy Approach (RTA) based on node behavior prediction for secure routing. It presents a behavior prediction algorithm for recognizing node behavior by differentiating among the unintentional transient errors and intentional malicious behavior, and the RTA mechanism which provides a method for node trust computation and a method for trust recovery. Experiment results show throughput improvisation against the malicious node intrusion. With increasing, malicious nodes in network RTA mechanism effectively predicted with an optimal packet loss and delay it attained prove the effectiveness of the mechanism.

Keywords: Reliability, Trustworthy, Behaviour, Secure routing, Mobile ad hoc network.

1. Introduction

Advances in wireless communications devices and networks provide instantaneous interconnectivity to build a temporary mobile ad hoc network (MANET). In these networks, each node acts as an intermediate router, and successful communication over a dynamic topology have no assurance of successful delivery. Even the dynamic paths found for routing are not guaranteed of not having any malicious nodes. The communication protocol used is designed with the assumption that all participants are adhering to the rules. However, in an unreliable communications environment, a malfunctioning user may be compromised or otherwise dishonest of network performance [1, 2]. Therefore, to ensure efficient use of resources, especially in wireless ad hoc networks, it is important to establish reliable communications where nodes depend entirely on cooperating with the secure path for successful packet transmission.

Most traditional approaches to network security are based on encryption methods. Unfortunately, these methods cannot handle malfunctions at the network media access control (MAC) layer. Selfishness and malicious behavior are classified in two major classes of malpractice being categorized [1, 3-5]. Selfish nodes always set goals to use more network and device resources, or intentionally generate false node information compared to normal nodes. Most selfish nodes block much of the communication channel, causing low bandwidth and reducing the device energy resources for decline routing packets. The overall communication operation is being targeted by the malicious node that can cause "congestion", "denial of service", "path fabrication", etc., [6-8]. It creates severe problems for communication in the presence of such kind of malicious node in the network [9].

The most conventional technique identifies the selfish and malicious node based on the packet drop but it's not always true as a node can have a different state of cause for the packet loss, and based on these prediction most this technique punished or avoid from the network. This avoidance or punishment will drop down the trust level a node and after a certain period, it is being removed from the network from the participation, which is the major drawback of the conventional technique. Even the impact of changing node behavior in practical communication solves the problem of harmless node isolation. Most of the previous approaches [4, 10] isolate nodes in the network based on two factorial assessments based on packet forwarding and request responses. This isolation increases network maintenance overhead, resulting in high instability and poor performance. In order to overcome these drawbacks this paper, propose a novel node behavior prediction mechanism. Behavior prediction is a strong factor to judge a node trustworthiness. It provides a node reliability and protection being declared as malicious simply based on packet drop. The strength of the proposal is to make the appropriate differentiation between the selfish, malicious and normal node to provide a trust and reliable node which will build a stable and secure network.

As the past study and analysis summarized that the node behaviour changes have a strong impact on the survivability of the nodes over the network. We proposed a Reliable Trustworthy Approach (RTA) which provide two prediction mechanism to simplify the survivability issues. We summarized the contributes of the paper as follows,

- It provides a generic model for categorizing node behaviour through determining the routing nodes actions and reactions independently to complete any communication operation between source and destination.
- The problem of behaviour prediction based on behaviour categorization addressed through a Semi-Markov Process, where each node behaviour probability is computed through monitoring node runtime behaviour actions.
- The problem of node trustworthiness is being addressed through behaviour probability prediction and its cumulative trust computation, where it recognize the trusted and malicious node efficiently.
- We suggest a strong trust recovery mechanism to regain the trustworthiness for the Reliable category (R) nodes. This provides a true enhancement for identifying the selfish and reliable node which support in improvising the network stability and retaining the node trustiness.

The remaining paper is organized as follows. Section-2 discusses the related research to the node behavior prediction and trust management approach. In next, the proposed node misbehaving prediction and RTA mechanism are presented in Section-3. The performance of the prediction and RTA mechanism are evaluated in section-4. Finally, Section-5 presents the conclusion of this paper.

2. Related works

The stability of the network in the literature is presented in different viewpoints by different researchers [1, 2, 10, 12-14]. These define the network traffic dimension associated with traditional communication networks and the survival concept of the network based on services, all of which are the primary concern for network reliability and node resilience [15]. We will discuss two key considerations related to network reliability, such as node behavior and trust management approaches for reliable communications and network stable performance.

2.1 Role of node behavior for trust changes

Several studies on the prediction of node behavior in literature have been discussed in [2, 5, 6, 12]. Thus, malfunctions and multiple failures of wireless nodes are encouraging new challenges to the survival of ad hoc networks and releasing results and its effect. Typically, the wireless node monitors neighbor node activity such as "packet forwarding", "packet drop", and "network link for successful packet delivery", however, these activities do not define node behavior. In [16], the authors discussed the effect of indirect observations on node propagation. A malicious node can lower the reliability of a normal node by propagating a negative message, while at the same time it can even recover node trust propagating a positive message also. Evaluating the trust scheme directly or indirectly in the recovery plan to avoid this false message detection can reduce the number of affected messages.

Previous work on trust restoration, are discussed in [5, 17, 18, 20, 21], which suggested that node restoration cannot be an important measure for node trust recovery, where nodes are discarded based on low dependency trust because it mostly measures the past behavior for trust calculation. Negative behavior nodes are isolated due to low trust and new untrusted nodes cannot join the network, so no new behavior is observed and the scope of node recovery is limited [16, 21]. Marchang et al. [3] propose an efficient plan for analyzing and optimizing the duration that IDS must remain active in MANET. A probabilistic model is proposed that uses cooperation between IDSs between neighboring nodes to reduce each activity time. Typically, IDS should always run on all nodes to supervise network activity. Z. Movahedi et al. [1]. It presents a holistic view of the various trust management frameworks that are suitable for MANET and can handle key existing attacks that mislead confidence calculations to mislead trust-based network operations, known as trust distortion attacks. It also suggests classification of key identified trust-traversal attacks based on how the node's reliability estimates for other nodes are distorted.

A node's behavior can be understood by evaluating past performance [22, 23]. Suppose that a node that is doing a positive action has a negative past in the past and can always assume that it behaves negatively in a reliable pathway. However, it is always fair that malicious nodes can prove their credibility and maintain network stability for a long time. CORE [13] is a system that evaluates node behavior based on direct and indirect observations from neighbor nodes. It observes only positive action messages associated with a specific task. It can compute it node trust using weighted trust mechanisms. In this case, the node gives a high weighted to the past actions as compared to the current action. The computed trust is used to isolate malicious nodes from the network for secure paths communication.

2.2 Trust-based security approaches

Many studies are performed in the consideration of trust for providing wireless network security [2, 6, 10, 12, 23, 24]. A neighboring node behavior monitoring approach for trust evaluation through a direct observation procedures is proposed in [25]. It describes the malicious behavior of a node depends on the number of packets forwarded for on receiving from the neighboring nodes. The source node computes the trust value with the support of direct detection of any data packet modification made by the intermediate node in the route [18]. The indirect approach considering trust observation made based on the messages transmitted by neighboring or ranges nodes to update positive or negative behavior of the node. This evaluation is considered to reconfigure trust for reconnection and to remove malicious nodes [13, 17, 26, 27].

To establish a secure and reliable routing in MANET a "Friend based Ad hoc routing using Challenges to Establish Security" (FACES) is proposed by S K. Dhurandher *et.al.* [28]. It defines a scheme for building a secure network based on a list of friends who share a list of nodes in a friend network. Friends are evaluated based on successful data transfers between nodes of other friends in the network. Each node periodically runs a process to get a list of shared buddies and build up the buddies' node responsibilities. Based on this periodic update, malicious nodes can be easily removed from the network. This approach does not need to observe neighboring transmissions for node reliability assessment. The disadvantage of this proposal is a high end-to-end delay due to computational overload and malicious behavior of the friend nodes, which can affect the entire buddy list, and communication and network stability.

A "Trust based Multipath Routing" (TMR) to provide trust-based routing using message security methods is proposed by P. Narula *et.al.* [8]. This approach reduces the number of data packets that are routed through low-trust nodes in cryptographic mode, so malicious nodes can destroy information and make good use of it. Routing strategies that use trust levels provide high scalability routing and avoid untrusted nodes in the route. This method assigns a unique trust level between -1 and 4. Level 4 defines the top level and -1 defines the lowest level of confidence between the nodes. The higher the reliability of a node, the greater the number of data packet routing. The assignment of trust depends on the direct observation of the neighboring nodes and all the praise received by any node of the network. Each encrypted data packet is divided into four parts and each part is sent to multiple available paths between the source and destination. It extends the DSR routing protocol to find the path from the source to the destination. The choice of path trust is calculated based on the new trust strategy. A node with trust level t can only transmit t data packet parts. When receiving a part, the destination node decodes the message part and joins it using the method defined in [8].

K. Ullah et al. [2] investigates trust and security issues to improve the security assurance of MANET. In conclusion, we propose a secure trust model that affects security assurance and critical adaptation of reliable communications and propose trust metrics based on the impulsive behavior of nodes in dynamic scenarios. S. A. Thorat et al. [4] compares trust-based cryptosystems for implementing MANET routing security. It describes the question of routing protocols based on a trust in the design detail MANET and the questionnaire about trust-based routing protocols for MANET. Jenitha T. et al. [24] proposes an improved mechanism for selecting a trusted node to participate in a key generation process for security group communication in a distributed environment of MANET.

A trust management based on negative and two-node behavior proposed by S. Bansal *et al.* known as "OCEAN" [26]. It reduces node trust for all negative messages and increases reliability in receiving all positive messages. Under a defined threshold trust it prepares a list of detected nodes sent from the channel. This information is used to avoid network nodes. Runs a timeout-based approach to removing nodes from the defect list. This recovery method does not take into account the current and past operating context of the node, which can affect the stability of the network. In [29], a "CONFIDANT protocol" which uses Bayesian reputation systems [30, 31] to calculate reliability based on node behavior evaluation is proposed. It periodically analyzes and uses a timeout based approach to node recovery. Although the negative behavior of a node in the current scenario directly affects the trust of the node, it is advisable to provide recovery opportunities, although it is expected that the node will have a negative history and would like to consider current requirements. It may be possible to network errors or malicious nodes due to affecting negative trust nodes.

V. L. Pavani et al. [34] proposed a secure trust management system (TMS) based on node behaviour predication algorithm to preserve high network stability and security for the reliable data delivery. It also considered the node behaviour different states and compute the node trust to preserve network security and reliability. The obtained results shows the improvisation in the throughput through effective prediction of node trust based on node behaviour changes.

This paper focuses heavily on observing changes in node activities for behavior prediction, collective trust calculations, and confidence recovery methods, which significantly reduces network overhead. Through extensive experiment analysis, this proposal provides an efficient approach to easily detect node security and malicious nodes in mobile ad hoc networks.

3. Reliable trustworthy approach

A reliable trustworthy approach (RTA) deal with prediction of node characteristic and identification to take part in the network [32]. As described above, the node behavior is can be an important factor for evaluating node trust. The nodes can activate in two ways: "positively" or "negatively". However, the cause of this behavior can be genuine or created virtually to interfere with network reliability. This proposal deal with a new node behavior prediction algorithm that estimates and predicts a behavior category that is used for effective decision-making method for node trust management and for reliable data transfer in MANET.

But the best of our knowledge, little work has been done to evaluate the characteristics of the node operations. Depending on the node connectivity and packet forwarding behavior from previous studies, the behaviors of neighboring nodes are described for reducing malicious nodes [14], [33]. But these work never analyzes the effect of node discard on the basis of some measures on the stability of the network. This proposal is targeted to solve this problem through the node trust recovery mechanism so that to maintain reliable and high throughput and, to maintain network stability.

3.1 Node behaviour prediction

The routing in MANET is depended on intermediate nodes collaboration and their trustworthiness. For the successful completion of communication operation, it is important to handle forwarding node efficiently [14]. According to their functionality, each forwarding and target node operates within the network accordingly. It determines their actions and reactions independently to complete any communication operation. This behavior is extended through a classification based on the assumption that all nodes in the network will operate in the following actions category:

- ***Reliable Category (R):*** This category of node action supports the best effort to deliver control and data packets while performing all routing rules and finds the right path for efficient routing.
- ***Un-Reliable Category (U):*** This category of node action makes the network is unstable may be as a result of "out of communication range", "high congestion", and "frequent link failures", etc.
- ***Malicious Category (M)***: This category of node action provides a suspicious activity to related

services, interrupting routing by periodically propagating "denial of service", "packet forwarding delays", "route manipulation", "positive or negative message", and so on.

- ***Selfish Category (S):*** This category delivers the best collaboration during route discovery. However, during routing operations, resource constraints are unreliable and do not respond to control messages in order to conserve resources intentionally.

In general actions, based behavior estimation algorithm utilizing the "Semi-Markov process" (SMP) has been proposed to accurately characterize the node behavior category predictions based on the above action categorization.

3.1.1 Semi-Markov process for node behavior prediction

The characteristic of wireless ad hoc network in real time can be altered at any point of time for different reasons unexpectedly. This causes the node behavior changes randomly at any time in the real-time network. It also might be caused by some attacks or lack of resource usage needed to maintain network links and packet forwarding. We measure the prediction of the behavior of different categories in related to the changes in the following behavioral observation.

- Because of the power loss and misinformation, they can affect the reliability nodes that can make them fail, and also due to other malicious attacks or selfishness which conserve its resources.
- Proper reconfiguration can also restore the credibility of selfish or malicious nodes. This reconfiguration can be counterproductive or fail due to a reduction in power resources.
- A malicious node can be a failed node, but if the malicious behavior is irregular, it is no longer considered unreliable or selfish.
- If the failed node routing activity can be periodically stable, the node can be trusted again.

Although there is no specific reason for behavioral changes in the above assumptions, this is the most common behavioral change observed in a wide range of network scenarios. To simplify this assumption for accurate behavioral prediction, we use the "Semi-Markov process" [11] to derive a mathematical model.

Let's considered a network region having N nodes as, W which consisting of different categories of nodes described above. It can represent as, $W = \{"R", "U", "M", "S"\}$. In particular to the time interval, T these nodes behavior can changes over time arbitrarily in W, which can be represented as,

$$W = \int_{n=0}^{N} T(Prob\,['R','U','M','S']) \qquad (1)$$

The prospect of these behavior changes can be predicted as, P_n at a course of time as, C_n and where, $C_n \in W$, can be presented as,

$$P_n = prob\,((P_{n+1} \rightarrow C_{n+1}) \mid (P_n \rightarrow C_n)) \qquad (2)$$

It will constitute the prediction utilizing a Markov chain [11] in a region of W using Eq. (2) for all the node N as P_n, and where $n = (0, 1, 2, ..., n)$. However, the dynamic behavior of the node changes completely in the observation chain at once. For example, if a node has low energy levels after a series of actions at a time and node stability is low, it might be selfish to preserve nodes. In conclusion, the node behavior of the current time interval of a node, $t(n)$ which can mean the future behavioral categories. This can be defined by means of a Semi-Markov method for behavior modeling [23] as,

$$T(B_{category}) = P_n, \forall C_{t(n)} \qquad (3)$$

where, $t_{(n)} \le t < t_{(n+1)}$. This can predict the probable changes of behavior using Eq. (3) for the most current behavior changes during a period t referring to a Semi-Markov behavior estimation process (SMP). This SMP process model can be used to describe a large scope of threats associated to node malfunctions and is related to node behavior classification.

Let's illustrate with an example as C_n is a current state of a node and after a time, t the behavior changes to $C_n = C_n + 1$, and it will be associated with a Semi-Markov value as,

$$M_{a,b}(C) = Prob\,(P_{n+1} = b, C_n \le c \mid P_n = a) = p_{ab}\, T_{ab}(c) \qquad (4)$$

where, "$p_{ab} = lim_{s \rightarrow \infty}$" and "$M_{a,b}(C) = Prob\,(P_{n+1} = b \mid P_n = a)$", represents the change of behaviour probability among the node a and b, and "$T_{jkab}(c) = Prob\,(P_n \le c \mid P_{n+1} = b, P_n = a)$", represents time period between two category changes among the node a and b.

Table 1. Probability of behaviour changes matrix

	R	*U*	*M*	*S*
R	**1**	1	1	1
U	1	**1**	0	0
M	0	1	**1**	0
S	0	1	1	**1**

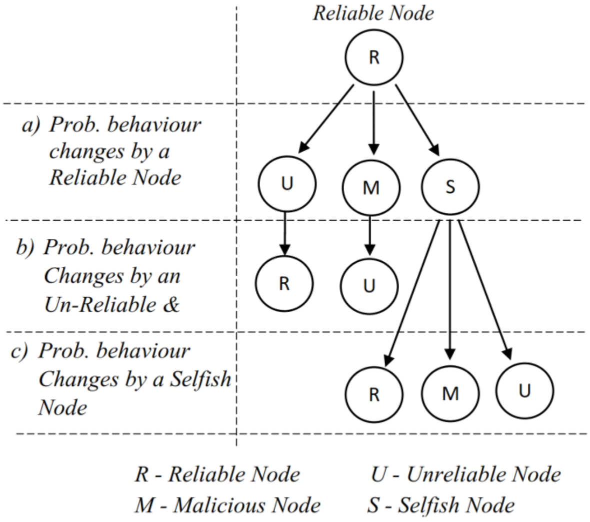

Reliable Node
R
a) Prob. behaviour changes by a Reliable Node
U
M
S
b) Prob. behaviour Changes by an Un-Reliable &
R
U
c) Prob. behaviour Changes by a Selfish Node
R
M
U
R - Reliable Node
U - Unreliable Node
M - Malicious Node
S - Selfish Node

Figure.1 Probability of behavior changes of different classes

On the basis of different classification behavior changes of a node, a probability matrix is presented in Table 1. On utilizing the probability of behavior changes matrix Table 1, we can estimate the behavior of a node, $T(B_{category})$ in associated to the current time of distribution, "T_{ab} *(t) = 1 | 0*". This can be presented in a model diagram as in Fig. 1.

If a node keeps unchanged while distributing its behavior and new behavior is observed, considering the one change at a time, the probability of change will be considered as *zero*. For example, in the case of a node reliability node, *R* it is possible to change the possible behavior category to *U*, *M* and *S* according to our assumptions matrices. Likewise, if a trusted node is observed Un-Reliable Node *U*, it can be changed its category to *R*, and similarly, a malicious node *M* can be changed to *R*, *M*, and *U* according to assumptions matrices.

If a node keeps unchanged while distributing its behavior and new behavior is observed, considering the one change at a time, the probability of change will be considered as *zero*. For example, in the case of a node reliability node, *R* it is possible to change the possible behavior category to *U*, *M* and *S* according to our assumptions matrices. Likewise, if a trusted node is observed Un-Reliable Node *U*, it can be changed its category to *R*, and similarly, a malicious node *M* can be changed to *R*, *M*, and *U* according to assumptions matrices.

This prediction of future definition models for the nodes behavior estimation based on assumption will be self-sufficiency. This predictive model of evaluation is utilized to calculate the node trust and recovery process of the proposed RTA mechanism to establish a secure and reliable communication.

3.2 Reliable trust prediction mechanism

RTA mechanism was proposed based on the probability of the behavior category of a node computation. All the nodes of the network assume that the system is reliable and value of the highest trust is configured as, $N_T = 1$. The credibility of reliable prediction based on behavior-based detection term as "RBP" and malicious behavior prediction term as, "MBP" along with the recovery process is discussed in this mechanism.

In RBP, we believe the present reliable behavior of nodes for a period and predicted its potential behavior using the semi-Markov process. For example, if a node current trust is 0.95 and it predicts possible behavior as reliable, then we can assume that this data packet will successfully forward by 90 percent. In order to fulfill a node on the order, it is considered as reliable and its trust value remains as previously predicted. In case it fails to fulfill the predictions performance for the required packet to deliver, then it is considered as malicious behaviors. Based on the number of observation for "RBPs" and "MBPs" using the above Semi-Markov Process a node probability trust, P_{Trust} is computed referring a "beta reputation system Bayesian formulation" [31] as given below, where RBP is total reliable behavior predicted and MBP is total malicious behavior predicted.

$$P_{Trust}(i) = \frac{RBP_i + 1}{RBP_i + MBP_i + 2} \qquad (5)$$

The P_{Trust} of the node describes what is the current node beliefs of a node in the right way and what is the behavior of a node is compatible with its past behavior which predicting the future behavior category. A low down P_{Trust} indicates that current collective trust value is less trustworthy and therefore it has to be avoided and the behavior of this node cannot be because it might be affected due to some attacks or any other cause, which requires a revision of the trust recovery.

An individual node trust calculations are typically based on individual activities performed, such as data forwarding and request processing [24].

The concept of P_{Trust} can operate in any way that calculates individual behavioral trusts or collective trusts (*CTs*). Based on individual behavior trusts, we define aggregation trusts to assess whether neighbouring nodes are malicious or not. Collective trusts are calculated from individual behavior trusts. Since there are many ways in which collective trust can be computed [12, 17-19], we present a collective trust of node *i* as "CT_i".

3.2.1. Collective trust computation

Node trusts are calculated based on individual total trusts (*TTs*) by the nodes over a period of time. Primarily, each node is assigned a maximum collective trust value of *1*. Since the confidence ranges for both P_{Trust} and *CT* are between 0 and 1, the best *CT* for a node can be calculated using Eq. (6) below.

$$CT_i = TT_i \times P_{Trust}(i) \qquad (6)$$

If the node's P_{Trust} is low enough, this method lowers the cumulative trust and drops it below the threshold. Therefore, P_{Trust} effects cumulative trusts that are independent of certain trust behaviors. Since Eq. (5) and Eq. (6) are calculated after every action change in which the node is used, you can invoke employment-based action-based recovery for node behavior analysis and trust restoration possibility.

3.2.2. Trust recovery

A "Recovery Factor" (RF) is also known as a "declining" or "forgetting" factor. This allows you to recover the trust value over time and provide a second opportunity for the node that is evaluated as malicious. Another way P_{Trust} is used is to calculate the RF of node *i* to control the leaving rate. The current trust value is used in conjunction with the current P_{Trust} value to calculate the *RF* so that the node can dynamically improvise the trust value of neighbor *i* according to its current trustworthiness. *RF* is estimated by using Eq. (7) and Eq. (8) to permit the trust to be transferred at the calculated rate, which is given by,

$$RF_i = \left(T_i^k \times P_{Trust}(i)\right) \times \alpha + 1.0 \qquad (7)$$

$$T_i^k{}_{after} = T_i^k{}_{before} \times RF_i \qquad (8)$$

where the $T_i^k{}_{after}$ and $T_i^k{}_{before}$ correspond to the individual k^{th} type of trust before and after the amendment of the i^{th} node and α represent value to control the tolerance of a scheme.

Since T_i^k is used to determine the RF_i,, each trust type can be recovered at different speeds. In Eq. (7) the value of α is $0 < \alpha \leq 1$, and it corresponds to a mechanism that permits the scheme designer to manage the acceptances of the scheme. If a system scheme needs to be firmly trustworthy, then it will be more tolerant to the smaller system. If P_{Trust} is low, since the behavior of the node is irregular, the redemption will take more time than the more predictable node. The Eq. (7) and Eq. (8) are calculated regularly using a time-based recovery mechanism.

4. Experiment evaluation

To assess the proposed RTA mechanism based on trust to meets the conditions specified in Section-3, and implement is made of a MANET routing environment. This experiment attempts to evaluate the possible actions and behavior of the source and intermediate nodes against the number of packets delivered to the target node for the number of packets sent from the source node. We demonstrate the effectiveness of P_{Trust} utilization modifying an AODV routing protocol for the simulation topology, node behavior prediction, collective trust and recovery methods.

4.1 Experiment setup

A simulative analysis was carried out using its API of GloMoSim. It provides a uniform distribution node and more practical movement prototypes. But, for otherwise specified, the speed is uniformly distributed in the random waypoint model using motion. A "Constant Bit Rate" (CBR) traffic is selected for 100 nodes, which are always maintained to keep traffic constantly maintained at every node in the network.

In addition, simulation, change their behavior according to the instructions node. For trusted nodes, AODV is used as a routing protocol while developing modified versions of AODV against malfunctioning nodes so that their behavior does not conform with the routing and forwarding rules identified in the standard. In particular, "selfish nodes" do not forward "RREQ" and "RREP" messages to others in the future; Malicious nodes forwarding RREQ and RREP messages but forward the data packet drop. The result is the average of the interest of several other malicious nodes in the simulation round. The simulation is set for 600 seconds so that the system is in a stable state. The default network settings are listed in Table 2.

Table 2. Simulation parameters

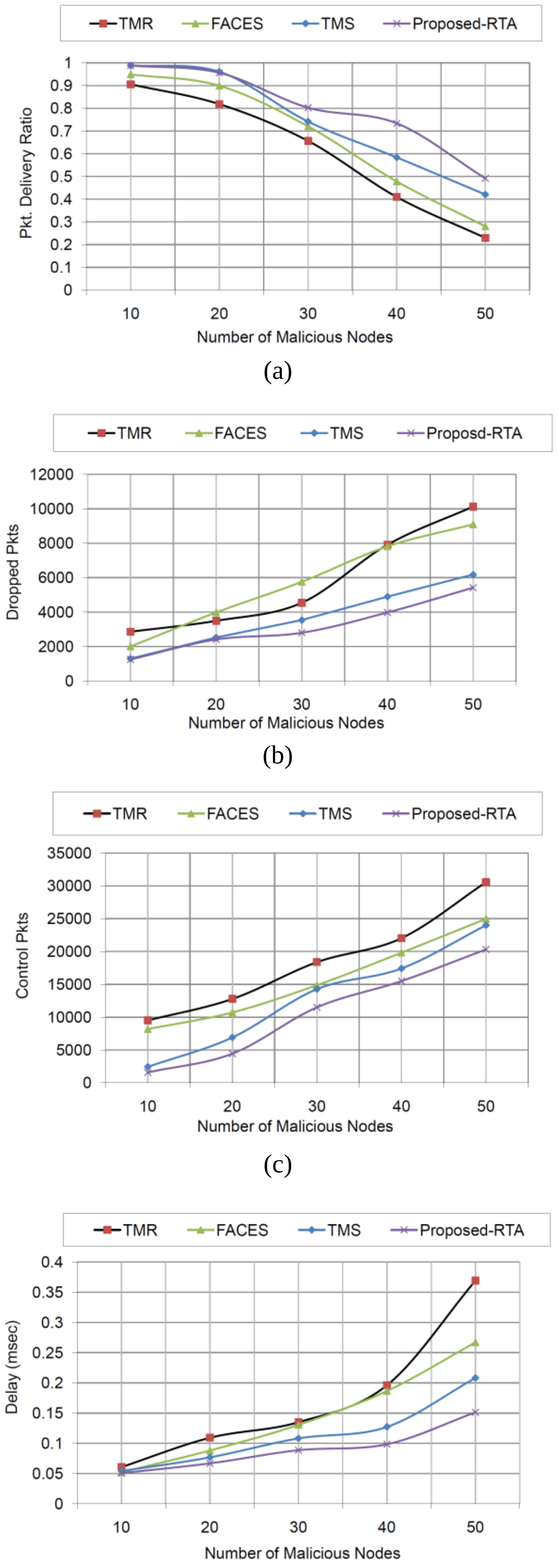
Configuration	Parameter Values
Simulation Time	1000s
Simulation Area	1500m X 1500m
No. of Nodes	100
Mobility	RWP
Mobility Speed	0 to 20 m/s
Pause Time	30s
Packet Size	512 bytes
CBR Rate	4pkts/s
Minimum P_{Trust}	0.7
Malicious Nodes	10, 20, 30, 40, 50
Trust threshold (P_{Trust})	0.5, 0.6, 0.7, 0.8, 0.9

4.2 Result analysis

In this section, we compare the protocol performance of proposed-RTA with TMR [8], FACE [28] and TMS [34] which are based on trust based routing mechanism. Primarily, we evaluate the performance varying malicious node and later varying the trust threshold(P_{Trust}) to measure the "Throughput", "Number of packets dropped", "Routing Overhead" and the "End-2-End Delay" based on the simulation parameter configuration given in Table 2.

4.2.1. Effect of malicious node

The effect of the malicious node is being examined over a trusted nodes and measuring the different parameter is discussed here. In Fig.2 (a) throughput performance is measured. The comparison results show an improvisation over TMR, FACE and TMS with varying numbers of malicious nodes variations. With the increase, malicious nodes affect the network throughput by dropping packets. The existing technique generally punishes the entire nodes in the route in case packet loss, which affects their trust even though they are innocent. RTA instead of punishing all it predicts each node behavior and its past collective trust to make a decision, which helps in to retain the path and improve the throughput. The accurate predictions allow nodes to join back to the network to stabilize and support better throughput. In Fig.2 (b), shows the number of packets discarded relative to the number of malicious nodes. With the increase of malicious nodes, TMR and FACES show high packet loss due to high denial by the malicious nodes, and the quick loss of routing path. The proposed RTA recovery scheme allows the node to restore its trust and handle high packet forwarding and fewer packet dropping.



(a)

(b)

(c)

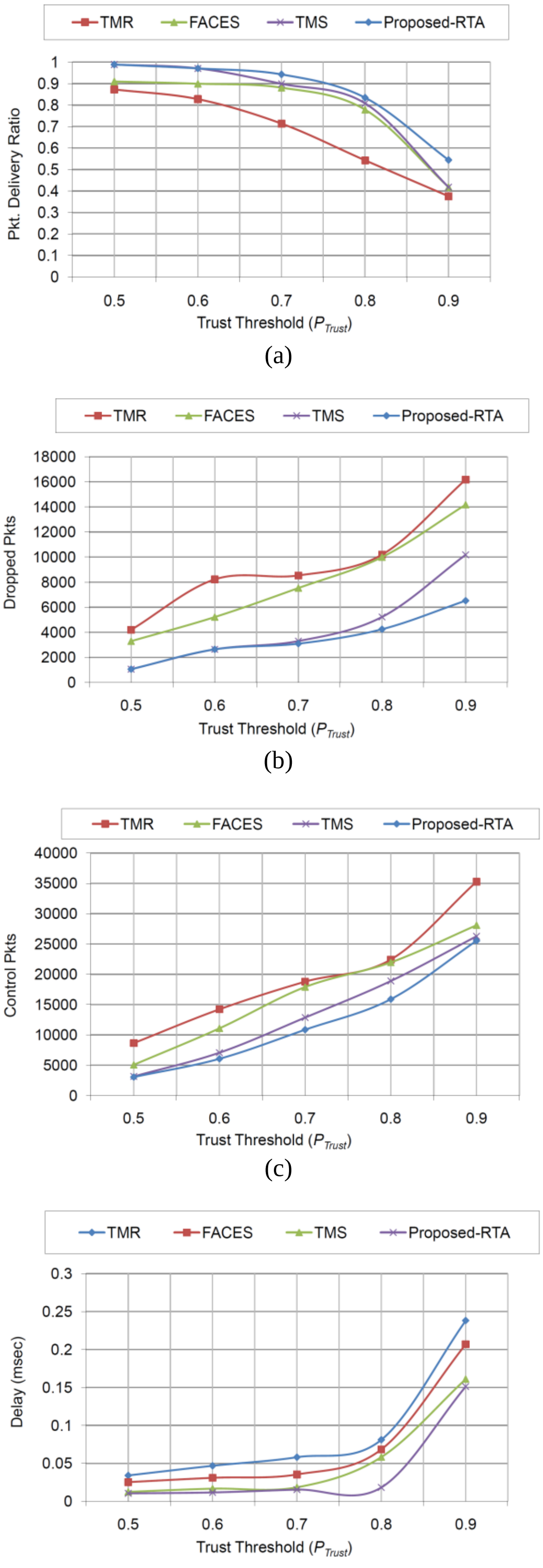
(d)

Figure.2 Effects of malicious node on the performance of various parameters: (a) throughput performance comparison, (b) packet drop comparison, (c) control overhead comparison, and (d) end-to-end delay comparison

In Fig.2 (c), shows the control overhead comparison of the protocol. All the protocols have reached a considerable level of overhead growth with increasing number of malicious nodes. The TMR shows high overhead in case of more number of a malicious node due to the large number of loss of data packets and the inability to recover any recovery scenarios, whereas the FACES, TMS and the proposed RTA show the difference in control overhead due to the retaining the reliable node based behavior prediction. In both protocols, the periodic node reliability assessment makes them retain the secure path and supports in packet loss and minimize the control overhead. In Fig.2 (d), shows the end-to-end delay performance comparison of the protocol. It describes the constant rate of end-to-end delay increments for all protocols as a result of changes in the number of malicious nodes. The RTA sends a smaller number of packets through a low-trusted node which helps to deliver packets with low delay. In case a high number of malicious getting a trusted node cause some delay and also might route through longer path causes a delay. Due to the maintenance of reliable and trustworthy nodes, the proposed RTA shows lower end-to-end latency in compared to the other, and in the case of high trusted node, it achieves 99% packet transmission with a minimum delay.

4.2.2. Effect of trust threshold

In this section, we evaluate the effect of Trust Threshold (P_{Trust}) on the trust bias and four performance measuring parameters as discussed. Here, we configure the network having 50% of the node as malicious and keeping another parameter as intact. In Fig.3 (a), shows the throughput comparison with varying Trust Threshold (P_{Trust}). In the case of low threshold, all the protocol shows the high throughput as high number of nodes can be in the low range of threshold but it unsafe for a long run as an unreliable node can easily maintain this threshold to retain in the network and affects the performance. In such, the increase of trust threshold (P_{Trust}) is needed. With the increase, P_{Trust} value TMR attains low throughput because it route data packets through low-trust nodes in cryptographic mode, whereas RTA, FACE and TMS shows a linearly low with increasing as both do periodically trust assessment and route the data with higher trust node. Higher trust nodes reduce with time as the impact malicious node cause the dropping of throughput at higher trust threshold (P_{Trust}).



(a)

(b)

(c)

(d)

Figure.3: Effect of trust threshold on the performance of various parameters: (a) throughput performance comparison, (b) number of packet drop comparison, (c) control overhead comparison, and (d) end-to-end delay comparison

In Fig.3 (b), shows a number of packet drops with varying trust threshold (P_{Trust}). As in Fig.3 (a) shows that increasing trust threshold (P_{Trust}) minimize the number of trusted node and may route the data in longer path cause loss packets and at lower P_{Trust} it shows low as a high number of a node available for routing but lower P_{Trust} unstable in the long run and causes more packet loss. In similarly, Fig.3(c) and (d) also shows an increase in control packets and end-to-end delay with increasing trust threshold (P_{Trust}) because of unavailability of higher trusted node, which impacts the routing performance. So, it infers that we should maintain an average trust threshold (P_{Trust}) to attain better throughput and low packet loss, control overhead and delay. To retain the trust threshold (P_{Trust}) one should efficiently monitor the node behavior and perform accurate trust computation to retain the innocent nodes in the network and also support the targeted node to recover their trustworthiness.

5. Conclusion and future works

This paper presents an RTA mechanism based on node behavior prediction using semi-Markov process. It targets the problem of innocent node isolation in practical communication based on the influence of node behavioral changes. As the conventional approaches mostly punish and isolate based on two-factor assessment based on the packet delivery and request reply which impact the network performance in terms of overload maintenance instability and low throughput.

The proposed RTA approach solves this problem through a reliable behavior prediction (RBP) and malicious behavior prediction (MBP) mechanism. It minimizes the unfairness of innocent node isolation through computing a probability model of isolation. It reduces the node isolation through the node collective trust calculation and a trusted recovery mechanism to improvise its trusts through a recovery factor. The experimental evaluation was performed in two different input. First, we evaluate evaluate the performance varying malicious node and later, varying the trust threshold values. We compare the obtained result with two trusts based protocol to identify the improvisation of the proposal. In both, the case of malicious node inputs and trust threshold inputs its outperform in all the evaluation measures in compare to comparison protocols.

The improvisation is achieved due to identifying the innocent node based on their behavior and past performance, instead of punishing the all the nodes in the route as conventional approaches do, which helps to retain the network for longer and improve the performance. In the future work, we would like to create this predictive method by analyzing the semantic changes in the negative and positive message spread by reliable and malicious nodes to build a more stable network over the network.

References

[1] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey", *IEEE Communications Surveys & Tutorials*, Vol. 18, No. 2, pp. 1287-1309, 2016.

[2] K. Ullah, R. Das, P. Das, and A. Roy, "Trusted and secured routing in MANET: An improved approach", *International Journal of IEEE Symposium on Advanced Computing and Communication*, pp. 297 - 302, 2015.

[3] N. Marchang, R. Datta, and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks", *IEEE Transactions on Vehicular Technology*, Vol. 66, No. 2, pp. 1684-1695, 2017.

[4] S. A. Thorat and P. J. Kulkarni, "Design issues in trust based routing for MANET", In: *Proc. of the 5th International Conf. on IEEE Computing, Communication, and Networking Technologies*, pp.1-7, 2014.

[5] M. Li, S. Salinas, P. Li, J. Sun, and X. Huang, "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Ad Hoc Networks: Detection and Defence", *IEEE Transactions On Mobile Computing*, Vol. 14, No. 6, pp/1203-1217, 2015.

[6] T. Shu and M. Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, Vol. 14, No. 4, pp. 813-828, 2015.

[7] G. Zhan, Shi W, Deng J, "Design and Implementation of TARF: A trust-aware routing framework for WSNs", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 2, pp. 184-197, 2012.

[8] P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust based multipath routing", *International Journal of Computer Communication*, Vol. 31, No.4, pp. 760-769, 2008.

[9] Chen, S. Garg and K. S. Trivedi, "Network Survivability Performance Evaluation: A Quantitative Approach with Applications in Wireless Ad-hoc Networks", In: *Proc. of*

International Workshop on ACM Modelling, Analysis, and Simulation of Wireless and Mobile Systems, pp. 61-68, 2002.

[10] A. Ahmed, K.A. Bakar, M.I. Channa, K. Haseeb, and A.W. Khan, "A Survey on Trust Based Detection and Isolation of Malicious Nodes In Ad-Hoc and Sensor Networks", *International Journal of Frontiers of Computer Science*, Vol. 9, No. 2, pp 280-296, 2015.

[11] B. J. Chang and S. L. Kuo, "Markov chain trust model for trust value analysis and key management in distributed multicast MANETs", *IEEE Transactions Vehicular Technology*, Vol. 58, No. 4, pp. 1846-1863, 2009.

[12] C. Xi, S. Liang, M.A.J. Feng, and M.A. Zhuo, "A Trust Management Scheme Based on Behaviour Feedback for Opportunistic Networks", *International Journal of China Communications*, Vol. 12, No. 4, pp. 117-129, 2015.

[13] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In: *Proc. of International Conf. on 6th Joint Working Communication, Multimedia Security*, pp. 107-121, 2002.

[14] R. A. Shaikh, H. Jameel, B. J. d Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks", *IEEE Transaction Parallel Distributed System*, Vol. 20, No. 11, pp. 1698-1712, 2009.

[15] J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length", *International Journal of Network Computer Application*, Vol.34, No.4, pp. 1138-1149, 2011.

[16] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks", *IET Information Security*, Vol. 6, No. 2, pp. 77 - 83, 2012.

[17] H. Xia, Z. Jia, L. Ju, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules", In: *Proc. of International Conf. on IEEE/ACM Green Computer Communication*, pp.124-130, 2011.

[18] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", *IEEE Communications Surveys & Tutorials*, Vol. 14, No. 2, pp. 279 - 298, 2012.

[19] G. Karame, I. Christou, and T. Dimitriou, "A secure hybrid reputation management system for super-peer networks", In: *Proc. of International Conf. on 5th IEEE Consumer Communication Network*, pp. 495-499, 2008.

[20] K. Paul and D. Westhoff, "Context-aware detection of selfish nodes in DSR based ad-hoc networks", In: *Proc. of International Conf. on IEEE Global Telecommunication*, Vol. 1, pp. 178-182, 2002.

[21] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", In: *Proc. of International Conf. on ACM Mobile Communication*, pp. 255-265, 2000.

[22] X. Mao and J. McNair, "Effect of on/off misbehavior on overhearing based cooperation scheme for MANET", In: *Proc. of International Conf. on Military Communication*, pp. 1086-109, 2010.

[23] T. Zahariadis , P. Trakadas, H.C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks", *International Journal of Wireless Personal Communications*, Vol. 69, No. 2, pp. 805-826, 2013.

[24] T. Jenitha and P. Jayashree, "Distributed Trust Node Selection for Secure Group Communication in MANET", In: *Proc. of the 4th International Conf. on Advances in Computing and Communications*, pp. 179-182, 2014.

[25] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices", *International Journal of Computer. Communication*, Vol. 33, No. 9, pp. 1086-1093, 2010.

[26] R. Venkataraman, M. Pushpalatha, and T. Rama Rao, "Regression-based trust model for mobile ad hoc networks", *IET Information Security*, Vol. 6, No. 3, pp. 131 - 140, 2012.

[27] W. Li, A. Joshi, and T. Finin, "Smart: An SVM-based misbehavior detection and trust management framework for mobile ad hoc networks", In: *Proc. of International Conf. on Military Communications*, pp. 1102-1107, 2010.

[28] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", *IEEE Systems Journal*, Vol. 5, No. 2, pp. 176-188, 2011.

[29] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol", In: *Proc. of International Conf. on 6th Annual*

Symposium on Mobile Ad Hoc Network Computer, pp. 226-236, 2002.

[30] Y. Chae, "Redeemable reputation based secure routing protocol for wireless sensor networks", *Master of Science Department Computer, University Rhode Island,* Tech. Rep. TR12-331, 2012.

[31] A. Josang and R. Ismail, "The beta reputation system", In: *Proc. of International Conf. on 15th Bled Electronic Commerce*, pp. 41-55, 2002.

[32] K. Paul, R.R. Choudhuri, and S. Bandyopadhyay, "Survivability Analysis of Ad Hoc Wireless Network Architecture", *International Journal of Mobile and Wireless Communications Networks*, Vol. 1818, pp 31-46, 2000.

[33] I. S. Abuhaiba and H. B. Hubboub, "Reinforcement swap attack against directed diffusion in wireless sensor networks", *International Journal of Computer Network Information Security*, Vol. 5, pp. 13-24, 2013.

[34] V. L. Pavani, B. Sathyanarayana, "A reliable data delivery using trust management system based on node behaviour predication in MANET", In: *Proc. of IEEE International Conf. on Applied and Theoretical Computing and Comm. Technology*, pp. 280-285, 2015.