Journal of Theoretical and Applied Information Technology
31st May 2019. Vol.97. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A BELIEF FORECASTING METHODOLOGY TO PRESERVE DATA SECURITY AND PRIVACY IN MANET ROUTING

[1] K. RAMESH RAO, [2]S. N. TIRUMALA RAO,[3]P. CHENNA REDDY

[1]Research Scholar, CSE, JNTUA, Anantapuramu (A.P), India
[2]Professor, Dept. of CSE, NarasaraoPeta Engineering College, Narasaraopeta, Guntur (A.P), India
[3]Professor, Dept. of CSE, JNTUA, Anantapuramu (A.P), India
Email-id: [1]karanamramesh@yahoo.com, [2]naga_tirumalarao@yahoo.com, [3]pcreddy1@rediffmail.com

ABSTRACT

The importance of data communication in wireless network demands a complete belief system through which the data security and privacy can be preserved during communication. Even the increase of the utilization of wireless data sharing especially in short-range communication or ad hoc network suffers from impersonation and DoS attacks. It is highly important to identify the belief nodes which supports the sort range or hop based communication to have a secure and privacy routing. In this paper, we propose a Belief Forecasting Methodology (BFM) to forecast the routing node about the believing nodes to improvise the data privacy routing in MANET. The goal of the BFM to protect the network from the malicious intruders and secure the data privacy during routing. It will compute the Belief Weight (BW) prediction based on the node activity and trustiness to decide the level of privacy of a node to support routing. The experiment simulation was performed through intruding malicious node in the network to evaluate the improvisation, and the result analysis suggested the effectiveness of the BFM to preserve the routing privacy in comparison of different evaluation measures.

Keywords: *Belief, Trust, Data Security, Privacy Routing, MANET*

1. INTRODUCTION

Mobile ad-hoc networks (MANETs) is an interconnection of multiple wireless nodes that can communicate with each other without using any network infrastructure or any centralized management. In order to promote multi-hop communication linking with the non-neighbor nodes, other nodes must function as routers. However, because of the "open and wireless media", "dynamic topology", "distributed and cooperative sharing of channels" and other resources such as "power and computational constraints", MANET is added high susceptible to security attacks than traditional wired and wireless networks. This limitation is a big challenge in finding trusted nodes and providing secure communications in MANETs. Many related methods are provided in this related (Z. Movahedi et al., 2016), (K. Ullah et al., 2015), (S. A. Thorat et al., 2014), (T. Shu et al., 2015), but the security based on trust computation is the lightest method and is very effective for limited resource communication. It also reflects the interdependence of a given node acting in a reliable manner and maintains reliable communication only with nodes highly trusted by the given node.

Many of these routing methods are supportive in character and depend on neighbors to route packets between contributing nodes (K. Paul et al., 2002). To achieve standard performance in these environments, the routing mechanism is strong for the active character of the environment, and the mobility of the nodes may cause a temporary disruption of existing links and discovery paths. A failed node tries to confuse the network without cooperating with other nodes (S. A. Thorat et al., 2014). The existence of a faulty node interferes with the ad hoc network by injecting incorrect routing updates, responding to "outdated routing information", "changing routing updates", or "advertising false routing information" and the "dynamic nature of ad hoc networks" (M. Li et al., 2015).

The most common technique is to identify selfish and malicious nodes based on packet loss, but this is not always the case, as nodes may have different states of packet loss reason, and based on these predictions most of these techniques are penalized or avoided The internet. This avoidance or penalty reduces the trust of a node and, over

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

time, is removed from the network, a major drawback of traditional technologies. The problem of inoffensive node isolation is solved even in the event of a change in node activity in the actual communication. Most previous approaches (S. A. Thorat et al., 2014), (Ahmed et al., 2015) isolated nodes in the network based on two factorial evaluations based on packet forwarding and request response. This isolation increases the overhead of network maintenance, resulting in high instability and poor performance. In order to overcome these shortcomings, a novel node activity prediction mechanism is proposed. Behavioral prediction is a powerful factor in determining the credibility of a node. It provides a node of reliability and protection is declared as malicious, just based on packet drop. The advantage of this approach is that it makes the proper distinction between selfish, malicious and normal nodes and provides a trusted node that builds a stable and secure network.

The belief system based on complete trust can be used to provide network security services such as receiving information quality evaluation, access control, authentication, detection of failed nodes and sharing of secure resources (T. Shu et al., 2015). Therefore, it is important to periodically evaluate the node's trust value based on some metrics and calculations. In this paper, we propose a node Belief Forecasting Methodology (BFM) to identify the node Belief Weight (BW) prediction based on the node activity and trustiness to be recognized by neighbor nodes in order to establish more secure and privacy routing in mobile ad hoc networks. Many of the existing trust computing techniques are discussed in (G. Zhan et al., 2012), (P. Narula et al., 2008), (Chen et al., 2002) and proposed in ad hoc networks with temporary actual results. In this suggestion, we calculate the node's runtime BW by trust predicting node runtime activity and trust. It ensures that the forwarding node has secure and private routing in MANET through trust characteristics supported on the BW level of the node.

The structure of this article is categorized as follows. In Section 2, we discuss the work related to the importance of node activities and the secure routing based on trust features. In Section 3, we explain the proposed belief prediction method and Section 4 describes the experiment and result evaluation. In the last section, we provide the conclusion of the paper.

2. RELATED WORKS

The stability of the network in the literature is put forward by different researchers from different perspectives as in (Z. Movahedi et al., 2016), (K. Ullah et al., 2015), (Ahmed et al., 2015), (Xi et al., 2015), (P. Michiardi et al., 2002), (C. Perkins et al., 2003). These define the network traffic dimension and service-based network survival concepts related to traditional communication networks, which are the primary considerations for network reliability and node resiliency (J. Wang et al., 2011). We discuss two key considerations related to network reliability as "trust management methods for node activity" and "reliable communications for the network stability".

2.1 Importance of Node Activities for Belief Forecasting

Several studies on node activity prediction in the literature have been discussed in (K. Ullah et al., 2015), (M. Li et al., 2015), (T. Shu et al., 2015), (Xi et al., 2015). As a result, wireless node failures and numerous malfunctions are creating novel challenges for the endurance of ad hoc networks and releasing the results and their impact. In general, wireless nodes monitor neighbor node activities such as "packet forwarding", "packet discarding" and "network link for successful packet transfer", however, these activities do not define node activities. In (N. Marchang et al., 2012), the authors discuss the impact of indirect observations on node propagation. Malicious nodes can reduce the reliability of normal nodes by spreading negative messages, and even restore the trust of nodes that propagate positive messages. Evaluating trust schemes directly or indirectly in a recovery plan to prevent this error message detection can reduce the number of messages affected.

Previous work on trust recovery was discussed in (M. Li et al., 2015), [17], (Z. Wei et al., 2014), (K. Paul et al., 2002), (S. Marti et al., 2000), which shows that node recovery cannot be an important means of trust recovery for nodes because it mainly measures the past of trust computation activity. Negative active nodes are inaccessible because of “low trust", new untrustworthy nodes cannot connect the network, so no recent activities are monitored and the range of node recovery is limited (N. Marchang et al., 2012) and (S. Marti et al., 2000). Marchang et al. (N. Marchang et al., 2017) proposed an effective plan to analyze and optimize the duration that IDS must remain active in MANET. A probabilistic model is proposed to reduce the time of each activity by using the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cooperation between IDSs between adjacent nodes. IDS should always run on all nodes to monitor network activity. Z. Movahedi et al. (Z. Movahedi et al., 2016) provide a holistic view of the different trust management frameworks that fit into MANET and can handle critical existing attacks, misleading the calculation of confidence to mislead trust-based network operations known as trust distortion attacks). It also proposes to classify the key-identified trust traversal attacks based on how the nodes estimate the reliability of other nodes.

Node activity can be understood by assessing past performance (X. Mao et al., 2010), (T. Zahariadis et al., 2013). Suppose a node that is taking positive action has a negative past in the history and can forever suppose that it behaves negatively on a credible path. However, malicious nodes have long proved their credibility and it is fair to maintain the stability of the network. CORE (P. Michiardi et al., 2002) is a system that evaluates node activity based on both direct and indirect observations by neighbors. It observes only positive behavioral information related to a specific task. It can use a weighted trust mechanism to calculate node trust. In this case, the node gives a higher weight to past actions than the current one. The calculated trust is used to isolate malicious nodes in the network for secure path communications.

2.2 Secure Routing Based on Trust Characteristics

In order to provide wireless network security, many studies consider trust (K. Ullah et al., 2015), (T. Shu et al., 2015), (Ahmed et al., 2015), (Xi et al., 2015), (T. Zahariadis et al., 2013), (T. Jenitha et al., 2014). In (J. Lopez et al., 2010) a neighbor node activity monitoring method for trust assessment through direct observation procedures is proposed. It describes a node's malicious activity depending on the number of forwarding packets it receives from its neighbors. The source node computes the trust value by directly detecting any packet modification made by the intermediate node in route (Z. Wei et al., 2014). An indirect method of considering trust observation is to update the positive or negative actions of a node based on messages transmitted by neighbor nodes or range nodes. This assessment is considered to reconfigure trust reconnection and remove malicious nodes (P. Michiardi et al., 2002), (Zhexiong Wei et al., 2014), (R. Venkataraman et al., 2012), (W. Li et al., 2010). In order to establish a secure and reliable routing in MANET and the trust management scheme proposed by Z.Wei et al. (Zhexiong Wei et al., 2014), the trust model has two components: "direct observation trust" and "indirect observation trust". Direct surveillance from the viewer node, the trust rate is imitative using "Bayesian inference", which is an indefinite interpretation when the complete probability model is able to characterize. On the other hand, indirectly observing second-hand information about neighbor nodes, also called observer nodes, using DST (Dempster-Shafer theory) to derive trust values, DST is another type of uncertainty inference that can be derived indirectly. By coming together with these two components in the trust model, a further precise trust value for the observation node in the MANET can be obtained.

P. Narula et al. (P. Narula et al., 2008) proposed a "trust-based multipath routing (TMR)" that uses a message security approach to provide trust-based routing (P. Narula et al., 2008). This approach reduces the "number of packets" routed during the "low-trust node" in cryptographic mode, so a malicious node can corrupt the information and make the most of it. Routing strategies using trust levels provide highly "scalable routing" and keep away from untrustworthy nodes in the route. This method assigns a unique trust level between "-1 and 4". Level 4 defines the top level, -1 defines the lowest confidence level between nodes. The higher the reliability of a node, the greater the number of packet routing. The distribution of trust mostly relies on the straight surveillance of neighboring nodes and all the good reviews received by any node in the network. Every encrypted packet is divided into four parts, each part of which is sent to multiple available paths between the "source and the destination". It extends the DSR routing protocol to find the path from "source to destination". The choice of path trust is supported through a new "trust schemes". A node of "trust level *t*" can only "transmit *t* packet" parts. When a part is received, the destination node decodes the message part and unites it with the method described in (P. Narula et al., 2008).

K. Ullah et al. (K. Ullah et al., 2015) investigated trust and security issues to improve MANET's security assurances. In summary, we propose a secure trust model that affects the security assurance and key adaptation of reliable communications and proposes a trust metric based on the impulsive act of nodes in a dynamic scenario. S. A. Thorat et al. (S. A. Thorat et al., 2014) Compare Trust Based Cryptosystems for MANET Routing Security. It illustrates the "trust-based routing protocol" in MANET design details. Jenitha T. et al. (T. Jenitha et al., 2014) proposed an improved mechanism for selecting trusted nodes to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

participate in the key generation process of security group communication in MANET distributed environment.

The trust management based on negative and two-node activities proposed by S. Bansal et al. it is called "OCEAN" (R. Venkataraman et al., 2012). It reduces node trust for all negative messages and increases the reliability of receiving all positive messages. Under a defined threshold trust, it prepares a list of detection nodes sent from the channel. This information is used to avoid network nodes. Run a timeout-based approach to remove the node from the defect list. This recovery method does not take into account the current and past node operating environment, which will affect the stability of the network. In (S. Buchegger et al., 2002), a "CONFIDANT protocol" based on Bayes reputation system is proposed to calculate the reliability based on node activity evaluation (Y. Chae et al., 2012), (Josang et al., 2002). It periodically analyzes and uses a time-out-based approach to recover nodes. Although the negative activity of a node in the current scenario has a direct impact on the node's trust, it is advisable to provide a recovery opportunity, though it is expected that the node will have a negative history and take into account current needs. It is possible to the network has bad or malicious nodes as it affects negatively trusted nodes.

Based on the above observation and the importance of node activities and trust characteristics for a belief system we proposed a belief forecasting methodology as discussed in the following section.

3. PROPOSED BELIEF FORECASTING METHODOLOGY

The proposed belief prediction method (BFM) assumes that there are "internal" and "external attacks" on the network, but most of the nodes in the network are "trustworthy". This procedure applies a "asymmetric cryptography" and provides a protected identification key "*sid_key*" for each node in the network. It uses this "*sid_key*" for the message encryption to prevent message fabrication.

3.1 Acquiring of Trust Certificate for Identity

Every node in the network has to acquire a protected "trust certificate" from a "trusted certification authority (CA)" to ensure its identity before joining the network. Security certificates that have been issued cannot be invalidated or terminated during the life of the network. If the node's trust value drops below the threshold, the certificate will be invalidated. This means that the legitimacy of the certificate determination be maintained until the credibility is continued In this process, we will be capable of locating the nodes that hold an illegitimately valid certificate and prevent the penetration of malicious nodes into the routing process.

The notations used in trusted identification certificates for a node Certificate as N_{cert} are denoted as,

Notation	Description
NCA_{ukey}	Node Trust certificate Public Key by CA
NCA_{pkey}	Node Trust certificate Private Key by CA
N_TA_{key}	Node trusted identification Key
N_{add}	Node Address
N_{ukey}	Node Public Key
N_{pkey}	Node Private Key

The certificate issued by a trusted CA is represented as,

$$N_{cert} = \boldsymbol{E_{TA_{pkey}}}[N_{add}, N_{ukey}, TA_{ukey}, E(N\_TA_{key})_{N_{pkey}}]$$

The certificate issued by the trusted CA is composed of the "CA public and Private key", "the node address" and "the public key and the private key of the node", and the node trusted identification code generated by the CA and encrypted by the node private key N_{pkey}. The entire certificate is encrypted with one "CA private key N NCA_{ukey}". The "CA public key" determination to be utilized to validate former node certificates.

3.2 Computational Process of Belief Weight (BW)

The proposed BFM approach performs the Belief Weight (BW) prediction computation as BWP_{value}, based on four parameters described as, Correctly authenticated as *Correct_Auth* (C_{Auth}), Incorrectly authenticated as *Incorrect_Auth* (IC_{Auth}), Successfully Packet Delivered as *Success_Pkt* (S_{pkt}) and Loss/Drop in packet delivery as *Loss_Pkt* (L_{pkt}). This parameter measures the following rate values which will be used for BWP_{value} computation.

- *Correct_Auth* (C_{Auth}) : It measures the number of value for a node successfully authenticated in producing for justification its identity.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- *Incorrect_Auth* (IC_{Auth}) : It measures the number of value for a node incorrect authenticated in producing for justification its identity.
- *Success_Pkt* (S_{pkt}) : It measures the number of value for a node successful packet delivery by a node.
- *Loss_Pkt* (L_{pkt}) : It measures the number of value for a node unsuccessful(loss or drop) packet delivery by a node.

These values are computed based on the regular monitoring of the communication process between source and the destination node. To compute the authentication measure a node asks its neighbor node to produce its identity for the authorization, on successful validation the *Correct_Auth* (C_{Auth}) is incremented by 1 if it fails then *Incorrect_Auth* (IC_{Auth}) value is incremented by *1*. Similarly, in case of the successful data delivery process, the node participated in the route for routing *Success_Pkt* (S_{pkt}) value is incremented by *1*, otherwise *Loss_Pkt* (L_{pkt}) is incremented by *1*.

This process of computation of each individual parameter can be represented as,

$$C_{Auth} = \sum_{i=0}^{n} Correct\ Authenticated \qquad S_{Pkt} = \sum_{i=0}^{d} Packet\ Delivered$$

$$IC_{Auth} = \sum_{i=0}^{n} Incorrect\ Authenticated \qquad L_{Pkt} = \sum_{i=0}^{d} Packet\ Loss$$

where,

n - Number of time identification is asked to produce during a communication cycle and,

d – Number of data packets transmitted during data routing through a particular node.

Utilizing these computed parameter C_{Auth} , IC_{Auth} , S_{pkt} and L_{pkt} values for each individual node we measure the two rate factors as, *Node Trust Rate* (NT_{Rate}) and *Node Packet Delivery Rate* (PD_{Rate}) based on the equation (1) and (2).

$$NT_{Rate} = \frac{(C_{Auth} - IC_{Auth})}{n} \times 100 \qquad (1)$$

$$PD_{Rate} = \frac{(S_{Pkt} - L_{Pkt})}{d} \times 100 \qquad (2)$$

Based on these two NT_{Rate} and PD_{Rate} rate values we compute the prediction of each node trust value as BFP_{value} using the equation (3). This value will be utilized for the final decision purpose during the communication by the source node and intermediate node for their next hops node.

$$BWP_{Value} = \frac{(NT_{Rate} + PD_{Rate})}{2} \qquad (3)$$

This BWP_{value} factor utilized as a source node which takes a decision using a threshold limit value for consideration of a node for communication or not. We will discuss the trust prediction routing mechanism in detail in the following section.

3.3 Privacy Routing using BWP

Effective data routing is the foremost goal of routing methods in ad hoc networks. The proposed protocol transmits data through determining routes discovered during route discovery after computing BWP values for each node. This protocol presupposes that the entire nodes in the network are initially trustworthy. The "trust value" is estimated supported by equation (3) described above.

The source sends the packet to the destination via the cached path. Send a confirmation on the receiving destination node for each packet received. Each node requires its neighbor nodes to generate a trust prediction key before sending a data packet. N_TA_{key} is encrypted using NCA_{ukey}. N_TA_{key} is validated before passing packets to the intermediate node. Upon successful authentication, *Correct_Auth* (C_{Auth})is incremented, and in the case of failure, *Incorrect_Auth* (IC_{Auth}) is added. This ensures that the source successfully transmitted the packet through the secure and trusted node. Communication between "source and destination" is initiated by opting for the best path from the route cache. Most favorable path choice is to depend on the "shortest" and "highest" 1st-hop node trust values associated with the source.

Table-1 Routing Table For Source Node

S-No.	Destination Route	1st-Hop	BWP_{value}
R1	1-2-7-10→D	1	0.4
R2	**3-6-8-11-10→D**	**3**	**0.8**
R3	4-5-9-7-12→D	4	0.4
R4	4-6-7-9-11→D	4	0.4
R5	3-2-5-7-10-12→D	3	0.8

For example, source node has five routes to destination D as given in Table-1 routing table. Although the initial route in the table is the "shortest", but the proposal chooses the 2nd route as the first hop of the second route with a high trust value. Routing based on the entire route trust is not

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

advisable because the trust of a "modest intermediate nodes" involved in the routing, possibly extremely low or only some nodes perhaps extremely high giving more packet loss and increased communication overhead to computational fare trust Link failed. In order to overcome this shortcoming, BF method is proposed to route the data packet to the node which has a high degree of trust for maintaining the route.

Table-2 Routing Table For Intermediate Node-3

S-No.	Destination Route	1st-Hop	BWP_{value}
R1	3-6-8-11-10→D	6	0.7
R2	3-2-5-7-10-12→D	2	0.6

The "intermediate node" pursues the identical method as the source node, it also follows a routing table as demonstrating in Table-2. The Node-3 have two forwarding hops according to the routing table illustrated in Table-2. Depend on the "trust value" computation node-6 transmits the "data packet" to node-2 instead of node-2. This option will carry on until the "data packet" is reached to the target. The recommended method improves packet delivery efficiency. Each intermediate node needs to transmit a "signature acknowledgment" to its preceding hop upon successful transmission of the packet to the subsequent hop. If the next hop is unsuccessful, the "intermediate node" transmits a "node error message" to the source and attempt the next accessible hop. If the "intermediate node" cannot route the entire hops, a "routing error message" is sent to the source. The source penalizes the complete node through reducing trust and keep away from those routes with these nodes in the future.

The source node maintains a sequence number table for the packets it sends. At any time, it accepts a confirmation, it keeps posting the trust factor entry for every node in the path sent by the packet. After confirming that the time source did not receive the acknowledgment, it determination presume that the packet was by no means perfectly transmitted and increase the "Node Trusted Rate (NT_{Rate})", and in the case of failure it penalizes the corresponding path by increasing its corresponding "Node packet delivery Node Rate (PD_{Rate})" value.

4. EXPERIMENTAL EVALUATION

To evaluate the proposed trust-based BF method, an implementation is configured in a MANET routing environment. The experiment attempts to evaluate possible activities and behaviors of the source and intermediate nodes, "the number of packets" transported to the target node for the number of packets forwarded from the source node. We demonstrate the effectiveness of using "BWP_{value}" for AODV routing protocols that modify simulation topology.

4.1 Setup

A GloMoSim's API being utilized for configuration and simulation the proposed mechanism. It provides a unified distribution node and a more practical prototype of the campaign. However, it is otherwise provided that the rate is evenly distributed over the moving random waypoint model. A Constant Bit Rate (CBR) traffic for 100 nodes keeps this traffic to maintain the traffic for each node in the network unchanged.

In addition, simulations change their activity according to the instruction nodes. For trusted nodes, AODVs are exploited as a routing protocol while developing a customized description of the AODV to prevent the failed nodes from making their activities inconsistent through the "routing and forwarding rules" identified in the paradigm. In particular, "selfish nodes" do not forward "RREQ" and "RREP messages" to earlier; malicious nodes transmitted "RREQ and RREP messages", excluding the forwarded packets are discarded. The result is the average interest of several other malicious nodes in the simulation wheel. The simulation is set to 600 seconds to keep the system in a steady state. Table 3 lists the default network settings.

Table 3. Simulation Parameters

Configuration	Parameter Values
Simulation Time (*sec*)	1000
Terrain Area	1000m X 1000m
Number of Nodes	100
Mobility Model	RWP
Mobility Speed (*m/s*)	0 to 20
Pause Time (*sec*)	30
Packet Size (*bytes*)	512
CBR Rate (*pkt/s*)	4
Avg. BWP_{value} Threshold	0.6
Malicious Nodes	10, 20, 30, 40, 50
Belief threshold (BWP_{value})	0.5, 0.6, 0.7, 0.8, 0.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2 Evaluation of Results

In this section, we compare the proposed BFM protocol performance to AODV (C. Perkins et al., 2003), TMR (P. Narula et al., 2008) and TMS (V. L. Pavani et al., 2015) based on the trust-based routing mechanism. First, we evaluate the malicious nodes with performance changes and then change in belief weight trust threshold (BWP_{value}) to measure the "Throughput", the "Number of dropped packets", the "Routing Overhead", and the "End-2-End Delay". Table 2 shows the simulation parameters Configuration.

A. Analysis of Malicious Activities

The effect of a malicious node is being examined for a trusted node and different parameters measured are discussed here. The throughput performance is measured in figure 2 (a). Comparisons showed that improper use of AODV, TMR and TMS had different numbers of malicious node changes. As the number of data increases, malicious nodes affect network throughput by discarding packets. The existing technique penalizes the entire nodes in a route, often with packet loss, affecting their trust even if they are innocent. Rather than penalize all nodes, FWM predicts each node's activity and past collective trust decisions, which helps preserve paths and increase throughput. Accurate prediction allows the node to return to network stability and support better throughput. In figure 2(b), the "number of packets discarded" relative to the "number of malicious nodes" is shown. As the number of malicious nodes increases, "TMR" and "AODV" illustrate higher packet loss rates due to the high reject rate of malicious nodes and the rapid loss of routing paths.

In figure 2(c), a comparison of control overhead for this protocol is shown. With more and more malicious nodes growing, all the protocols have reached a considerable "level of overhead" growth. Due to the large "number of packet" losses and the inability to recover any recovery scenario, TMR shows a high overhead with a large number of malicious nodes. Since AODV, TMS and the proposed BFM exhibit the proper control overhead to preserve reliable, Node activity forecast. In both protocols, periodic node reliability assessments allow them to keep secure paths and support packet loss and minimize control overhead.

In figure 2(d), the "end-to-end delay performance" of the protocol is shown. It describes the invariable rate of "end-to-end delay" for all protocols due to changes in the number of malicious nodes. BFM sends a smaller number of packets over low-confidence nodes, which helps to send packets with low latency. If we have a lot of malicious nodes get some delay, and may route longer path will lead to delay. Due to the maintenance of reliable and trusted nodes, the proposed BFM has a lower end-to-end delay compared to other nodes, while in the case of highly trusted nodes, 99% of the packets are transmitted with a minimum delay.

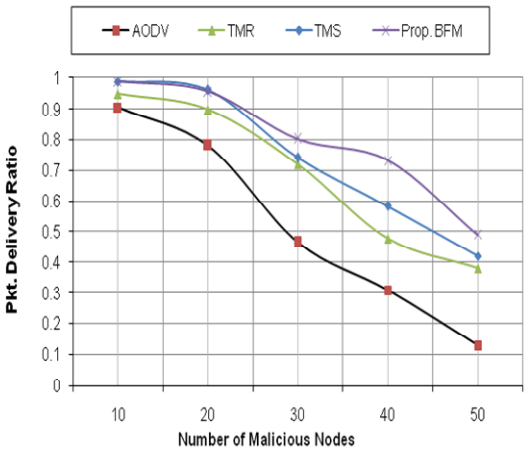

Fig. 2(A) Throughput Performance Comparison

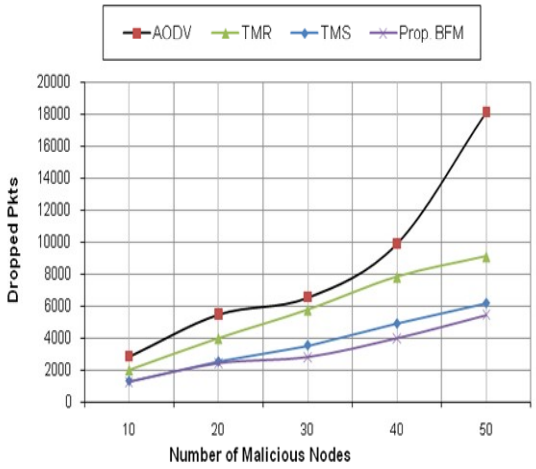

Fig.2(B) Packet Drop Comparison

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

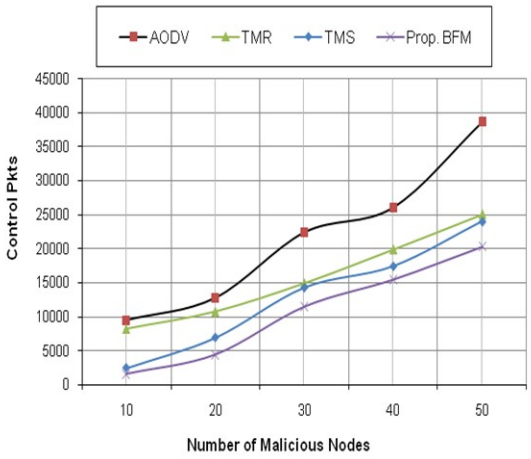

Fig. 2(C) Control Overhead Comparison

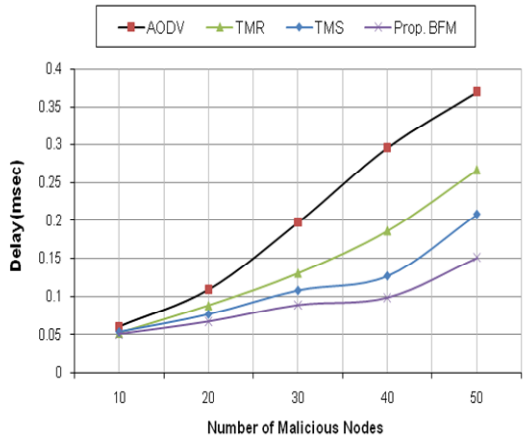

Fig. 2(D) End-To-End Delay Comparison

Figure.2: Effects of Malicious Node on the Performance of various Parameters

B. Analysis of Belief Weight Threshold (BWP_{value})

In this section, we evaluated the impact of the "Belief Weight Threshold (BWP_{value})" on trust bias and the four performance measurement parameters. Here, we configure the network with 50% nodes to be malicious and leave the other parameters unchanged. In Figure-3 (a), a comparison of throughput with varying "BW Threshold (BWP_{value})" is shown. At low thresholds, all protocols exhibit high throughput because a high number of nodes can be in the low threshold range, but this threshold can easily be kept due to unreliable nodes to stay in the network and impact unsafe in the long-term performance. As such, the increase of BW threshold (BWP_{value}) is needed. With the increase, BWP_{value} value TMR attains low throughput because it routes data packets through low-trust nodes in cryptographic mode, whereas BFM, AODV and TMS show 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 BW threshold (BWP_{value}).

In Figure.3(b), shows a number of packets drops with varying BW threshold (BWP_{value}). As in Fig.3(a) shows that increasing BW threshold (BWP_{value}) minimize the number of trusted node and may route the data in longer path cause loss packets and at lower BWP_{value} it shows low as a high number of a node available for routing but lower BWP_{value} unstable in the long run and causes more packet loss.

In similarly, Figure.3(c) and (d) also shows an intensify in "control packets" and "end-to-end delay" with increasing BW threshold (BWP_{value}) because of unavailability of the higher trusted node, which impacts the routing performance. So, it infers that we should maintain an average BW threshold to attain better throughput and low packet loss, control overhead and delay. To retain the BW threshold (BWP_{value}) one should efficiently monitor the node activity and perform accurate BW computation to retain the innocent nodes in the network and also support the targeted node to recover their trustworthiness.

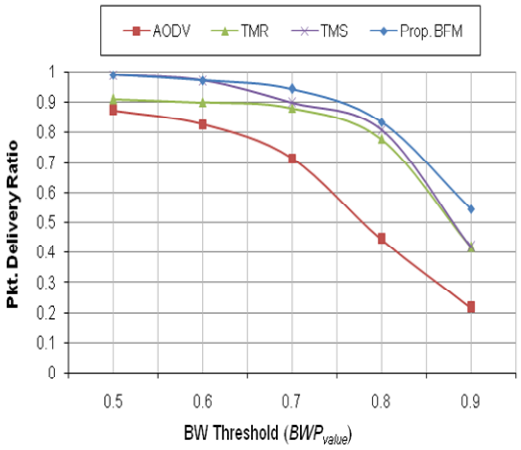

Fig. 3(A) Throughput Performance Comparison

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

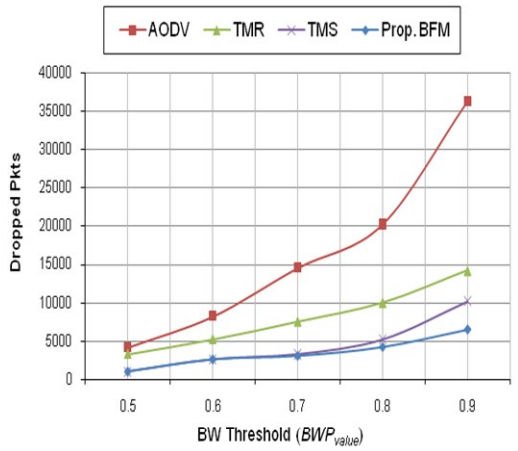

Fig. 3(B). Number Of Packet Drop Comparison

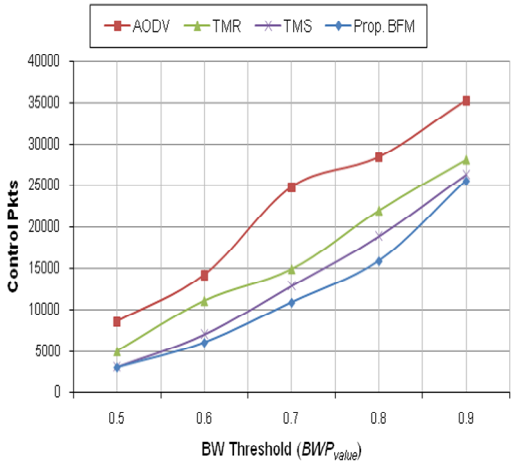

Fig. 3(C) Control Overhead Comparison

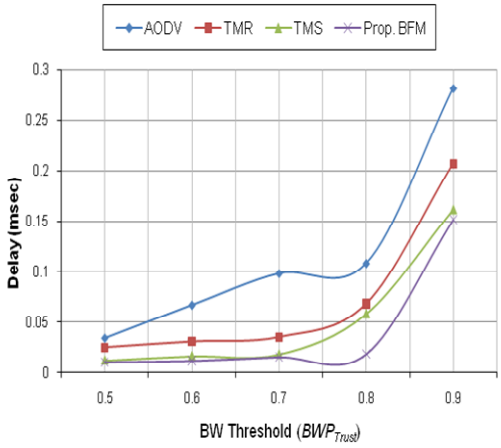

Fig. 3(D) End-To-End Delay Comparison

Figure.3: Effect Of Trust Threshold On The Performance Of Various Parameters

5. CONCLUSION

This paper presents a Belief Forecasting Methodology (BFM) based on node activity prediction. It targets the problem of innocent node isolation in practical communication based on the influence of node activities 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 BFM approach solves this problem through a Belief Weight (BW) prediction. It minimizes the unfairness of innocent node isolation through computing a probability model of isolation. It reduces the node isolation through the node collective BW calculation. The experimental evaluation was performed in two different input. First, we evaluate the performance varying malicious node and later, varying the BW 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 evaluate to comparison protocols. The inventiveness is achieved due to identifying the innocent node based on their activity 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 with faithful and malicious nodes to construct a more stable network over the network.

REFERENCES:

[1] Ahmed, K. A. Bakar, M. Ibrahim Channa, K. Haseeb, 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, Volume 9, Issue 2, pp 280-296, 2015.

[2] 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, Sept. 2002.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] Perkins, E. Belding-Royer, and S. Das, *"Ad hoc On-Demand Distance Vector (AODV) Routing,"* IETF RFC 3561, Jul. 2003.

[4] 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.

[5] G. Zhan, Shi W, Deng J, *"Design and Implementation of TARF: A trust-aware routing framework for WSNs"*, International Journal of IEEE Transactions on Dependable and Secure Computing, Vol. 9(2), pp. 184-197, 2012.

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

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

[8] 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.

[9] 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.

[10] 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.

[11] K. Paul, R.R. Choudhury, 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.

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

[13] 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"*, International Journal of IEEE Transactions on Mobile Computing, Vol. 14, No. 6, June 2015.

[14] N. Marchang, R. Datta, S. K. Das, "*A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks", International Journal of IEEE Transactions on Vehicular Technology*, Volume: 66, Issue: 2, Pages: 1684 - 1695, 2017.

[15] N. Marchang, R. Datta, *"Light-weight trust-based routing protocol for mobile ad hoc networks"*, International Journal of IET Information Security, Vol. 6, Issue: 2 Pages: 77 - 83, 2012.

[16] 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.

[17] 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 Science Direct Computer Communication, Vol. 31, 2008.

[18] 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.

[19] S. A. Thorat, P. J. Kulkarni, *"Design issues in trust-based routing for MANET"*, In Proc. of International Conf. on IEEE Computing, Communication, and Networking Technologies, DOI: 10.1109/ ICCCNT.2014.6963101, November 2014.

[20] 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.

[21] 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"*, International Journal of IEEE Systems, Vol. 5, No. 2, 2011.

[22] 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.

[23] R. Venkataraman, M. Pushpalatha, T. Rama Rao, *"Regression-based trust model for mobile ad hoc networks", International* Journal of IET

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Information Security, Vol. 6, Issue: 3, Page(s): 131 - 140, Sept. 2012.

[24] T. Jenitha, P. Jayashree, *"Distributed Trust Node Selection for Secure Group Communication in MANET"*, In Proc. of International Conf. on IEEE 4th Advances in Computing and Communications, DOI: 10.1109/ICACC.2014.50, 2014.

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

[26] T. Zahariadis , P. Trakadas, HC. Leligou, S. Maniatis , P. Karkazis, *"A novel trust-aware geographical routing scheme for wireless sensor networks"*, International Journal of Wireless personal communications, Vol. 69(2), pp. 805-826, 2013.

[27] V. L. Pavani, B. Sathyanarayana, *"A reliable data delivery using trust management system based on node behavior prediction in MANET", I*EEE International Conf. on Applied and Theoretical Computing and Comm. Technology (iCATccT), Pages: 280 - 285, 2015.

[28] W. Li, A. Joshi, 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.

[29] Xi, S. Liang, MA. Jian Feng, MA Zhuo, *"A Trust Management Scheme Based on Behaviour Feedback for Opportunistic Networks", International Journal of China Communications*, Volume: 12, Issue: 4, Page(s): 117 - 129, April 2015.

[30] 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.

[31] 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.

[32] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang and Peter Mason, *"Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning"*, IEEE Transactions on Vehicular Technology, Vol. 63, No. 9, November 2014.

[33] Z. Movahedi, Z. Hosseini, F. Bayan, G. Pujolle, "Trust-Distortion Resistant Trust Management Frameworks on Mobile Ad Hoc Networks: A Survey", *International Journal of IEEE Communications Surveys & Tutorials*, Volume: 18, Issue: 2, Pages: 1287 - 1309, 2016.

[34] Z. Wei, Helen Tang, F. Richard Yu, Maoyu Wang and Peter Mason, *"Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning"*, IEEE Transactions on Vehicular Technology, Vol. 63, No. 9, November 2014.