Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

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

REPETITIVE TRUST MANAGEMENT AND ADVERSARY DETECTION FOR DELAY TOLERANT NETWORKS

[1]C.ASHOK BABURAJ,[2] DR. K. ALAGARSAMY
[1]Associate Professor,Department of Master of Computer Application, K.L.N College of Engineering, Pottapalayam, Sivagangai,India.
[2]Associate Professor, Madurai Kamaraj University, Madurai, Tamilnadu, India.
E-mail: [1]ashokbaburaj@yahoo.com, [2]alagarsamymku@gmail.com

ABSTRACT

Delay Tolerant Networking (DTN) program is an emerging technology that can facilitate access to information when secure end-to-end paths cannot exist. DTNs may be turn into vulnerable during the legitimate nodes may compromise and the attacker modifies or alters the delivery constraints of the node. DTN makes use of persistence within the network nodes along with the mobility strategy to overcome the delay for connectivity. The existing trust management protocols are not an effective approach to handle the security attacks. In this paper, an efficient approach termed as a Repetitive Trust Management (RTM) and Adversary Detection is proposed to handle the Byzantine attacks in DTNs. It takes into consider the reputation values among the nodes participated in the data transmission. Bipartite graph is utilized to represent the subset of the nodes participate in the network. Trust Based Management Classifiers is presented which uses the Bloom filter to check the hash functionalities between the nodes. Here, threshold mechanism is used to enhance the secure communication in DTNs. The experimental results proves that the proposed scheme detects the malicious nodes and recovers the message within short duration of time.

Keywords: *Adversary Detection, Bipartite graph, Bloom filter, Byzantine attacks, Delay Tolerant Networks (DTNs), Multi hop transmission, and Repetitive Trust Management (RTM).*

1. INTRODUCTION

Delay / Disruption Tolerant Network (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. These networks have the unique features of irregular connectivity, that makes the packet routing is quite different from the other wireless networks. Also, end-to-end conversations are not always possible on a direct routing path through the network due to the irregular network connectivity. Thus, routing is realized by multi-hop transmissions and explores simultaneous communications among the nodes. DTN technology makes use of persistent storage within network nodes, along with the opportunistic use of mobility, to overcome the disruptions to connectivity. A traditional TCP/IP network depends on the stable end-to-end connectivity – an identifiable path all the way to the destination. Some of the applications of DTNs consist of emergency response, vehicular-to-vehicular communications, military, healthcare and tactical sensing. In the Department of Defense's wireless tactical networks, connectivity is often disrupted by terrain, weather, jamming, movement, or destruction of nodes. Such disruption makes it impossible to determine a path, halting the flow of data. Due to the limitation in bandwidth and buffer space, DTNs are vulnerable to flooding attacks. The DTN setup is mainly appealing in large Mobile Adhoc Networks (MANETs) that have no fixed infrastructure. In these networks, performance scalability is attained by exploring the mobility of the nodes and the intermediate nodes required to store, carry and forward the data packets to the corresponding destination. Due to the limitation in bandwidth and buffer space, DTNs are vulnerable to attacks.

Trust and reputation are the vital requirements for most environments. In MANET DTN environments, it is important to choose a trustworthy node as a next hop among all encountered nodes to minimize the delay for a message to reach a destination node and maximize the packet delivery ratio. Due to the lack of knowledge of the network topology and the end-to-

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

end path, routing, unicasting, broadcasting and multicasting becomes harder even with no packet deletion. In MANET, the attacker nodes may cause various attacks against DTNs to degrade the performance of the network. One of the most serious attacks is caused by Byzantine i.e. inside attacker. In these attacks, one of the legitimate nodes may compromise and fully controlled by the attacker node. In order to prevent the Byzantine attack, the network is equipped with the highest level security mechanisms.

In this paper, a repetitive based trust management technique is proposed for adversary detection. This system depends on the repetitive decoding of low-density parity check codes among bipartite graphs. Without the help of central authority, the system accurately calculates the reputations among the network nodes within a short time. RTM reduces the impacts of the Byzantine attackers. Rating table is created for each Service Providers (SPs) to know about the details about the nodes and to provide authentication for secure transmission from source to destination. The rating table is periodically updated based on the feedback response. Here, bipartite graph is used, which composed of the collection of all the network nodes represented as bit vertices. The threshold value is utilized to know about the adversary node and the normal node. The existing system depends on single hop transmission, whereas the proposed scheme utilizes the multiple hop communication between source and destination. The multiple intermediate nodes are used for data transmission in a secure manner. Hence RTM removes the attacker nodes and formulate the secure network.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the detection of adversary nodes and possible security mechanisms used in DTNs. Section III involves the detailed description about the proposed Repetitive Trust Management and Adversary Detection scheme. Section IV presents the performance analysis. This paper concludes in Section V.

2. RELATED WORK

This section deals with the works related to the detection of adversary nodes in DTNs and the possible trust based routing protocols for secure transmission from the source to destination. *Zhu et al* proposed a probabilistic misbehavior detection scheme. It was designed for secure DTN routing against efficient trust formation. The Trusted Authority (TA) was used to judge the nodes behavior. It was based on the collected routing evidences and probabilistically checking. This scheme corresponds to the detection probability determined by the trust of the users [1]. *Zhou et al* proposed an autonomic group key management scheme for deep space DTN. A logical tree was based on one-encryption key multi decryption key protocol. Each legitimate user in the DTN had a same competence to modifying the public key encryption with their decryption key as a key management center. Due to the lack of key management center support, rekeying can be attained by a local leaving or joining user. This rekeying message cost was half of the Logical Key Hierarchy (LKH) [2]. *Zhang et al* presented a node trust evaluation strategy in Mobile Adhoc Networks (MANET). This model was based on multi-dimensional fuzzy and Markov Single factor system Cloud Grey Model i.e. SCGM (1, 1) model. Also, the authors [3] presented a pattern for making predictions.

Xia et al designed a dynamic trust prediction model to validate the trustiness among the nodes. It was detected based on the nodes historical behavior using the extended fuzzy logic rules prediction. In order to provide a secure routing, the trust prediction model was merged with the source routing mechanism. So, this routing methodology was termed as Trust based Source Routing protocol (TSR) [4]. *Xia et al* proposed a trust management model for MANET based on two models. The models were subjective trust evaluation model and trusted routing model. The model was based on the analytic hierarchy process and fuzzy theory. In the subjective trust evaluation model, the credibility among the nodes was calculated based on the analytic hierarchy process theory and fuzzy logic rules prediction method. The model was termed as Fuzzy Trusted Dynamic Source Routing (FTDSR) protocol [5]. *Ren et al* presented various methods to detect the wormhole attacks. of that, a detection mechanism was presented that exploits the existence of a forbidden topology on the network. The random way point and zebranet mobility models were presented to evaluate the detection mechanism [6].

Miao et al investigated the unwillingness of nodes to participate in mobile DTN routing. The hops maintain the rational behavior called selfishness and their wariness of disclosing private mobility information. The classification approach was presented to deal with the selfish behavior of the nodes [7]. *Xiaofeng et al* introduced an anti-localization routing protocol. This protocol achieves the anonymous delivery in DTNs. The probability of a data source being localized and

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

maximize the destinations probability of receiving the message were attained. It protects the senders location privacy with the help of message fragmentation and forwards the individual segment to different receivers [8]. *Li et al* proposed an identify-based signature scheme with batch authentication (ISBA) for Delay Tolerant Mobile Sensor Networks (DTMSN). An online and offline signature was designed with batch authentication in order to decrease the computational cost. The data delivery mechanism was incorporated to increase the number of messages for each batch authentication [9].

Kumar et al presented a Probabilistic Trust Aware Data Replication strategy in Vehicular Delay Tolerant Networks (VDTNs). It was especially designed for video streaming applications. A Data Replication Tree (DRT) was constructed to show all the nodes with their interconnection were starting from the source to the destination. It increases or decreases the size of the network based on when the node leaves or joins the network. A Replica Cost function (RCF) was used to manage the data replica. It composed of three types of costs like Data Communication Cost (DCC), Data Storage Cost (DSC) and Data Update Cost (DUC). A Trust Calculation Metric (TCM) was used by considering the aforementioned criteria's among the nodes for data replica placement. The replica location and data replication algorithms with read and write were established trust between the nodes [10]. *Johnson et al* proposed a cryptographic based authentication method. This method does not rely on network administrator's availability. At the same time, post network authentication communicates with the set of process by the recipients even the absence of connectivity [11].

Jia et al proposed a Dynamic Virtual Digraph (DVD) model. It was designed for public key distribution study by extending graph theory. A public key distribution scheme was used for pocket DTN based on two-channel cryptography [12]. *Djamaludin et al* proposed a decentralized trust system for autonomous DTN. A public key distribution model was based on the web of trust principle. A simple Leverage of Common Friends (LCF) trust system was employed to establish initial trust in autonomous DTN [13]. *Dini et al* presented a reputation based protocol for contrasting black holes. Each node maintains the repetition of forwarding nodes. The reputation protocol was composed of three mechanisms namely acknowledgement, node lists and aging. The mechanisms make the communication was capable of adapting to the changing operating conditions of a DTN [14].

Dhurandher et al proposed a Friend based Adhoc routing using Challenges to Establish Security (FACES) algorithm to provide secure routing in MANET. This system has been composed of a network of friends in real life scenarios. The friend lists were used to provide a list of trusted nodes to the source node through which data transmission takes place. The nodes included in the friend list were rated based on the amount of data transmission among the nodes in the network. The friendship among the nodes with the other nodes was obtained by the share your friends process. The process occurs periodically in the network. Challenges were used to gather the information about the malicious nodes i.e. attacker nodes [15]. *Cho et al* designed a trust management protocol. This protocol was used in the mission group communication system in MANET. The hierarchical modeling techniques were used based on stochastic petrinets. The trust among mobile nodes was critical for team collaborations without any previous interactions for mission driven group communication system in combat zone situations. The optimal length of a trust chain among nodes in a trusted web that generates the trust levels without revealing risk based on a tradeoff between trust availability. A trust metric for mission driven group communication systems was defined to reflect the unique characteristics of trust concepts [16].

Chen et al proposed a class of integrated social and Quality of Service (QoS) trust based routing protocols in MANETs. The trust evaluation in the routing protocol considers the QoS properties and social trust properties to calculate the other nodes encountered. A stochastic Petri net model was utilized to describe heterogeneous mobile nodes with the various social and networking behaviors [17]. *Bo et al* proposed the concept of trust to Adhoc networks. The concept was built by a simple trust model to evaluate the neighbors forwarding behavior. The trusted opportunistic forwarding model was designed by choosing the trusted and highest priority candidate forwarder. A Minimum Cost Routing (MCOR) algorithm was formulated [18]. *Natarajan et al* proposed a method for resource misuse attack detection in DTNs. Here, two types of resource misuse attacks were studied namely breath attacks and depth attacks [19]. *Talati et al* offered various trust methods and trust based routing protocols to provide trustworthiness of the neighbor nodes [20].

Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

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

3. REPETITIVE TRUST MANAGEMENT AND ADVERSARY DETECTION (RTM)

The proposed methodology considers the DTN environment is structured with no centralized authority. The nodes located on the network can communicate through multiple indirect hops. The main two objectives of this proposed trusted mechanism includes:

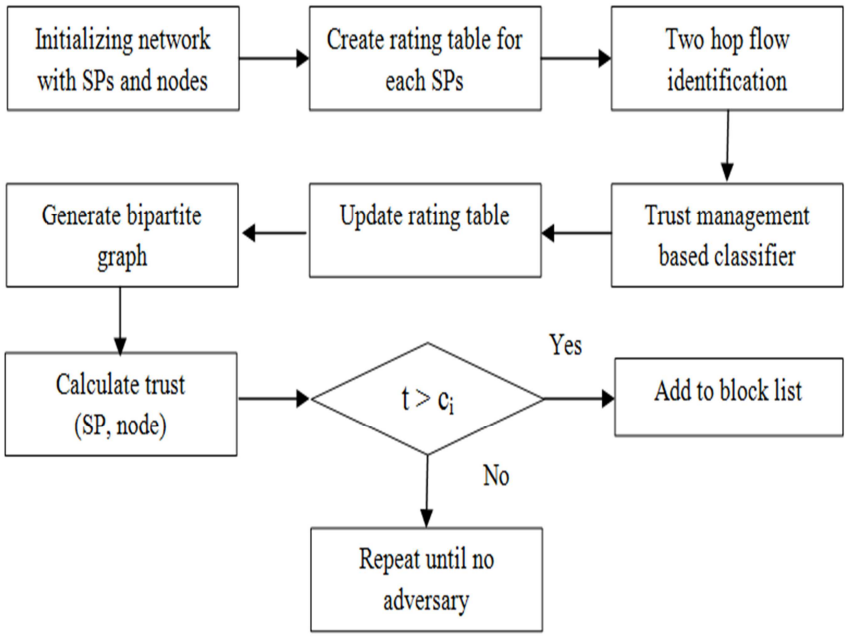


Fig.1.Structure of proposed Repetitive Trust Management and Adversary Detection

Fig.1. describes the Repetitive Trust Management and Adversary Detection scheme. Here, t denotes the threshold value and c_i denotes the trustiness calculation for all nodes i

a) Calculating the reputation among the peers based on the feedbacks from the raters.

b) Estimate the trustiness among the raters by analyzing their feedback about SPs.

This methodology is inspired by the traditional iterative trust management mechanisms; while traditional systems are depend on the single hop communication. Whereas the proposed system utilizes the multiple indirect hops for data transmission. The overall process of the proposed Repetitive Trust Management and Adversary Detection Scheme is depicted in Fig.1. The network is initialized with the SPs and the nodes. For each SPs, rating table is created. The rating table contains the subset of nodes has collected sufficient feedbacks. Bad mouthing and Ballot stuffing are the most common attacks usually occurred for any trust and repetitive management system.

3.1 Trustiness Calculation

The trustiness among the nodes can be calculated directly and indirectly based on eqn (1) and eqn (2). Consider T_n is the global reputation of *n*th SP, T_{mn} denotes the rating of the peers about the SP, it is estimated whenever the transaction is completed among two nodes.

$$T_{mn} = R_m.W(\delta_{sf} + \delta_{tf} + \delta_{pf}) + IDT_{mn} \quad (1)$$

$$IDT_{mn} = \frac{\sum_{v \in S} D_{v,n} * D_{m,v}}{D_{m,v}} \quad (2)$$

Here, R_m denotes the report/rating trustiness of peer m, δ_{sf} denotes the total number of success communications, δ_{tf} denotes the total number of times the transmission occurs, δ_{pf} denotes the number of trust communications, W denotes the weight, T_{mn} denotes the trust value between the node mn $D_{m,v}$ and $D_{v,n}$ denotes the number of nodes located on the path and IDT_{mn} denotes the indirect communication trust.

Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

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

3.2 Iterative Detection with Judge Node

A *judge node* is elected during the initialization of the network. The judge node monitors the SPs behavior and performance. A judge node can create the own rating about itself and also create a rating about another network node. The judge node is used to collect and aggregate the feedbacks about the nodes. Each judge node maintains a rating table whose entries are used to store the ratings about the network nodes. Due to mobility, the judge node waits for a long time to communicate and calculate its ratings about all the nodes. To overcome this difficulty, the Repetitive Trust Management and Adversary Detection scheme is proposed in this paper. The rating table entries are denoted with the help of bipartite graph. The bipartite graph may consist of one check vertex i.e. the judge node and some of the bit vertices i.e., the subset of all the nodes located on the corresponding network. Hence, the judge node can receive the feedbacks to calculate the ratings with high confidence.

The ratings results binary reputation values as '0' or '1'. A node which has the reputation value '0' can be detected as malicious nodes. Whenever two nodes start an interaction, they may sometimes exchange their reputation values. The proposed methodology assumes that the judge node does not have any knowledge about the witness node and it treats all the nodes equally. This technique is a simple and efficient technique to detect the malicious nodes. The ratings otherwise represented as a non-binary reputation values.

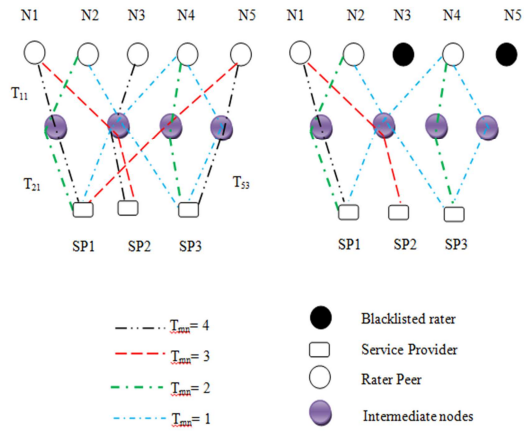


Fig.2. Example of RTM

3.3 Raters Trustiness

The raters values ate periodically updated using the set of all previous blacklists based on beta distribution. During the initial time slot, each rater is set to the value as 0.5.

If the rater r is blacklisted then R_r is decreased based on the following equation

$$\varphi_r(t+1) = \bar{\lambda}\varphi_r(t) + (c_r + 1 - \gamma)^{\delta} \quad (3)$$

Else

$$\phi_r(t+1) = \bar{\lambda}\varphi_r(t) + 1 \quad (4)$$

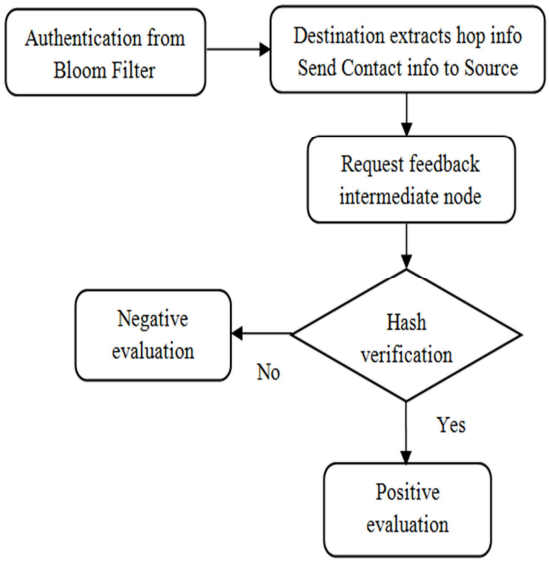
Here, $\bar{\lambda}$ denotes the fading parameter, t is the time taken, δ is the penalty factor for the corresponding blacklisted raters. where, $\varphi_r = 1, \phi_r = 1$ is fixed.

3.4 Trust Management Based Classifier

The proposed trust management system uses the Bloom filter for authentication. The destination node extracts the hop information from the received packet and forwards the contact information to the source node. The feedbacks are collected from all the intermediate nodes participate in the data transmission. The hash function is used to verify that whether the intermediate nodes are trusted one or not. Based on the hash function the nodes trustiness is evaluated which is shown in fig.3.

3.4.1 Bloom filter

Bloom filter is a space-efficient probabilistic data structure, which is used to check whether the node or an object belongs to a particular subset or not. A bloom filter represents the set S = $\{s_1, s_2 \ldots s_n\}$ for n items which is described by a vector of m bits. Initially all the values are set to 0. The filter uses the hash functions h_1, $h_2 \ldots h_k$ to map the items to a random integer across a range between 1…m regularly.



Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

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

Fig.3. Trust Management Based Classifier

For each item *s* in *S*, the bloom address is defined called *Bloomaddress(s)*. The address consist of $h_i(s)$ for $1 \leq i \leq k$ and the bits ϵ *Bloomaddress(s)* is set to 1 while inserting *s*. Whenever the set S is represented as a Bloom filter, it is necessary to judge whether an element $s \epsilon$ S , it needs to check whether all the hashed element bits $h_i(s)$ are set to 1. If it is possible, then *s* is a member of *S*. otherwise, assume that *s* is not a member of *S*. It is obviously known that the bloom filter results a false positive F due to the hash collisions. The probability of the false positive is obviously the probability that none of the *k* selected bits after training in the filter is still set as '0'. Consider *l* denotes the proportion of bits. It is fixed as '0' after the elements *I* have been inserted it implies

$$F = (1\text{-}g)^k \quad (5)$$

Here, g is the expected value and j items are entered. By hashing each *k* items the probability is maintained as zero,

$$g' = (1 - \frac{1}{i})^{kj} \sim e^{\frac{-kj}{i}} \quad (6)$$

This is the predicted value of g. Then, the false positive rate can be approximately calculated as

$$a = (1-g)^k \sim (1-g')^k \sim (1 - e^{\frac{-kj}{i}})^k \quad (7)$$

a denotes the approximated value, c and d are the intermediate nodes. To find the number of k functions k^* that minimizes,

$$k^* = \ln 2 \frac{m}{n} \quad (8)$$

It leads to the intuitive output that exactly half which is set to 1 when the optimal number of hash functions is chosen. Each function is assumed to be independent each other and map the items range between 1 to *m*. The structure is attractive when N>> *n*.

4. PERFORMANCE ANALYSIS

The proposed model is simulated and implemented with 50 raters and 15 SPs. The SPs work is to monitoring and managing the nodes on the network. The rating table is calculated based on the trustiness calculation among the nodes. During the initialization time, it provides reliable ratings to increase the trustiness values before the attackers attack the transmission. The proposed system performance is evaluated based on the following metrics: Packet Delivery Ratio, Malicious Node Detection Ratio, Mean Absolute Error (MAE) and execution time. The experimental results shows that the proposed scheme is effectively detect the adversary nodes than the existing scheme.

4.1 Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of number of genuine packets received by the destination with the number of genuine packets transmitted by the source. The proposed Repetitive Trust Management (RTM) results better packet delivery ratio when compared with the exiting Iterative Trust and Reputation Management (ITRM) [21] mechanism. It is depicted in the following fig.4

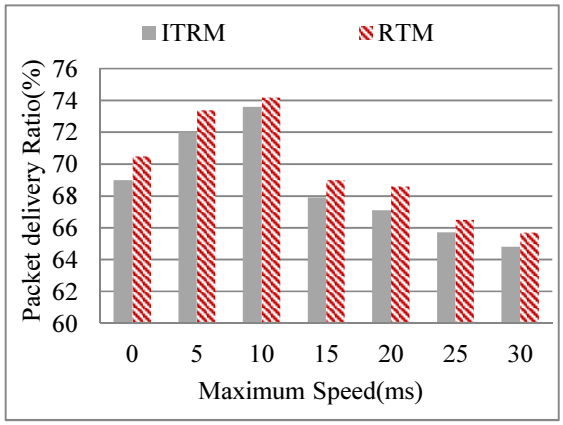


Fig.4. Packet Delivery Ratio between RTM and ITRM

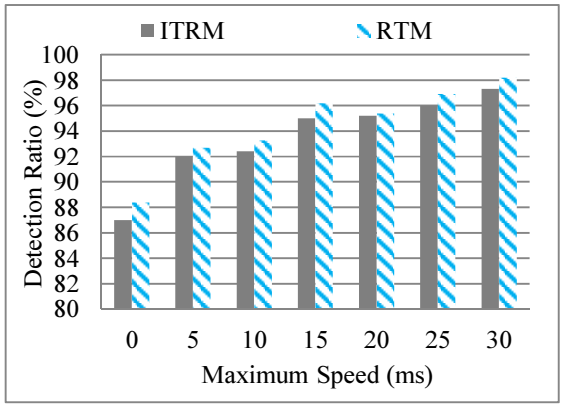


Fig.5. Malicious node detection ratio between RTM and ITRM

4.2 Malicious Node Detection

Fig.5. show that the malicious node detection ratio correlates with the node speed. The proposed RTM

Journal of Theoretical and Applied Information Technology
31st March 2014. Vol. 61 No.3

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

detects the malicious nodes better than the existing ITRM scheme.

4.3 Mean Absolute Error (MAE)

MAE is a quantity used to measure about the close forecasts or predictions for the eventual outcomes. It is estimated based on the following equation.

$$MAE = \frac{1}{n}\sum_{x=1}^{n}|a_x - b_x| \quad (9)$$

Where $|a_x - b_x| = |d_x|$, a_x is the prediction and b_x is the true value and n is the total number of iterations.

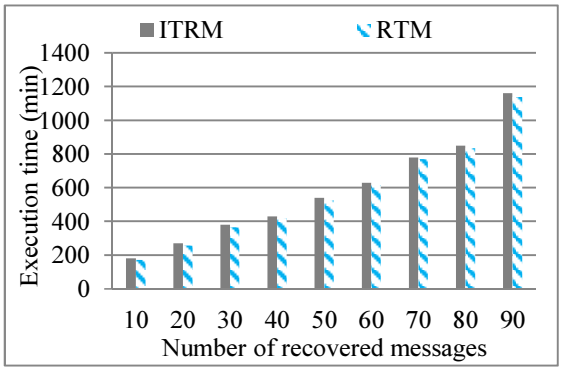


Fig.6. Mean Absolute Error

The performance of RTM is validated in terms of MAE is shown in fig.6. It is computed based on the reputation values which are validated by the judge node.

4.4 Recovered Message

The recovered message is estimated across the time which is shown in fig.7. It shows that the proposed RTM scheme takes less time to recover the message. The resulted values are tabulated in TABLE I.

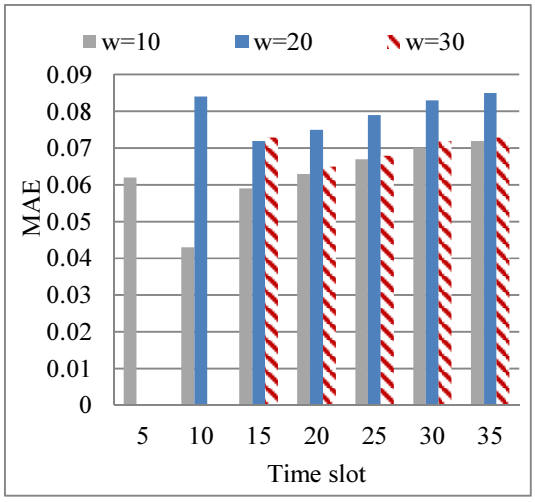


Fig.7. Recovered messgae vs Time

TABLE I EXECUTION TIME ANALYSIS

Number of recovered messages	Time taken for ITRM (ms)	Time taken for RTM (ms)
10	180	174
20	270	259
30	380	368
40	430	421
50	540	526
60	630	618
70	780	772
80	850	836
90	1160	1139

4.5 MAE for Bad Mouthing

The resulted values for MAE between ITRM and RTM is shown in fig.8. From that, it is obviously shows that the proposed scheme results better than the existing ITRM.

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

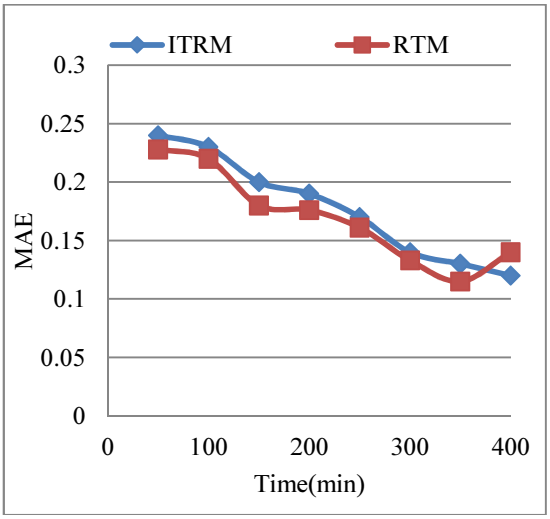


Fig.8. MAE for Bad Mouthing between ITRM and RTM

5. CONCLUSION AND FUTURE WORK

In this paper, an efficient Repetitive Trust Management and Adversary Detection scheme is introduced. The proposed scheme provides secure environment for data transmission from legitimate source to legitimate destination with the help of legitimate intermediate forwarding nodes. The proposed trust mechanism permits each node to calculate the trustworthiness among the nodes. The performance of the proposed RTM is evaluated with the existing iterative trust management mechanism. The proposed RTM scheme detects the Bad mouthing attack and prevents the data from these attacks. The result shows that the proposed scheme effectively detects the malicious nodes and performs better in terms of packet delivery ratio, mean absolute error and execution time. The performance are monitored and determined that the proposed model can performs better than the existing ITRM.

In future, the proposed structure can be analyzed with some other advanced security mechansims and utilize the best resulting security mechanism to protect the network from black hole attacks.

REFERENCES

[1] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks," *Parallel and Distributed Systems, IEEE Transactions on,* 2013.

[2] J. Zhou, M. Song, J. Song, X.-w. Zhou, and L. Sun, "Autonomic Group Key Management in Deep Space DTN," *Wireless Personal Communications,* 2013, pp. 1-19.

[3] F. Zhang, Z.-P. Jia, H. Xia, X. Li, and H.-M. Sha Edwin, "Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM (1, 1) model," *Computer Communications,* vol. 35, 2012, pp. 589-596.

[4] H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Networks,* 2012.

[5] H. Xia, Z. Jia, L. Ju, and Y. Zhu, "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory," *Wireless Sensor Systems, IET,* vol. 1, 2011, pp. 248-266.

[6] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting wormhole attacks in delay-tolerant networks [Security and Privacy in Emerging Wireless Networks]," *Wireless Communications, IEEE,* vol. 17, 2010, pp. 36-42.

[7] J. Miao, O. Hasan, S. B. Mokhtar, L. Brunie, and K. Yim, "An investigation on the unwillingness of nodes to participate in mobile delay tolerant network routing," *International Journal of Information Management,* vol. 33, 4// 2013, pp. 252-262.

[8] X. Lu, P. Hui, D. Towsley, J. Pu, and Z. Xiong, "Anti-localization anonymous routing for Delay Tolerant Network," *Comput. Netw.,* vol. 54, 2010, pp. 1899-1910.

[9] W.-j. Li, K.-f. Zheng, D.-m. Zhang, Q. Ye, and Y.-x. Yang, "Efficient identity-based signature scheme with batch authentication for delay tolerant mobile sensor network," *The Journal of China Universities of Posts and Telecommunications,* vol. 20, 8// 2013, pp. 80-86.

[10] N. Kumar and J. Kim, "Probabilistic trust aware data replica placement strategy for online video streaming applications in vehicular delay tolerant networks," *Mathematical and Computer Modelling,* vol. 58, 7// 2013, pp. 3-14.

[11] E. Johnson, H. Cruickshank, and Z. Sun, "Providing Authentication in Delay/Disruption Tolerant Networking

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

(DTN) Environment," in *Personal Satellite Services*, ed: Springer, 2013, pp. 189-196.

[12] Z. Jia, X. Lin, S.-H. Tan, L. Li, and Y. Yang, "Public key distribution scheme for delay tolerant networks based on two-channel cryptography," *Journal of Network and Computer Applications,* vol. 35, 5// 2012, pp. 905-913.

[13] C. I. Djamaludin, E. Foo, and P. Corke, "Establishing initial trust in autonomous Delay Tolerant Networks without centralised PKI," *Computers & Security,* vol. 39, Part B, 11// 2013, pp. 299-314.

[14] G. Dini and A. Lo Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network," *Ad Hoc Networks,* vol. 10, 9// 2012, pp. 1167-1178.

[15] 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," *Systems Journal, IEEE,* vol. 5, 2011, pp. 176-188.

[16] J.-H. Cho, A. Swami, and I.-R. Chen, "Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks," *Journal of Network and Computer Applications,* vol. 35, 2012, pp. 1001-1012.

[17] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Integrated Social and QoS Trust-Based Routing in Delay Tolerant Networks," *Wireless Personal Communications,* vol. 66, 2012/09/01 2012, pp. 443-459.

[18] W. Bo, H. Chuanhe, L. Layuan, and Y. Wenzhong, "Trust-based minimum cost opportunistic routing for Ad hoc networks," *Journal of Systems and Software,* vol. 84, 2011, pp. 2107-2122.

[19] V. Natarajan, Y. Yang, and S. Zhu, "Resource-misuse attack detection in delay-tolerant networks," in *Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International*, 2011, pp. 1-8.

[20] M. Talati, S. Valiveti, and K. Kotecha, "Trust Based Routing in Ad Hoc Network," in *Communication and Networking*. vol. 120, T.-h. Kim, T. Vasilakos, K. Sakurai, Y. Xiao, G. Zhao, and D. Ślęzak, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 381-392.

[21] E. Ayday and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks," *Mobile Computing, IEEE Transactions on,* vol. 11, 2012, pp. 1514-1531.