ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

DETECTION AND DEFENSE MECHANISM FOR MALICIOUS NODE IN MOBILE AD HOC NETWORK USING CLUSTER & REPUTATION SCHEME

Dr. M. Manimekalai M.Sc.,PGDCA.,M.Sc (IT).,M.Phil (CS).,Ph.D(CS)
Professor, Director and Head, Department of Computer Science, MCA and IT & Applications,
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

S. Annie Philomina
Research Scholar, Department of Computer Science
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

Abstract

Mobile Ad hoc Networks (MANET) are infrastructure less networks which provide multi-hop wireless links between nodes. The main applications of MANET in real time environment are military and emergency areas where the fixed infrastructure is not required. It is a temporary communication infrastructure network for quick communication with minimal configuration settings among the group of nodes. The security is one of the primary concerns in MANET. The malicious nodes in MANET environment degrade the performance of the network.In this paper, a novel cosine similarity based clustering and dynamic reputation trust aware key generation (CSBC-DRT) scheme is proposed. For better faced clustering, a cosine similarity measure is estimated for all the nodes on the network. Based on the similarity measure among the nodes, the network nodes are clustered into disjoint groups. The Reputation Trust Model (RTM)is built in this proposed scheme. Here, an improved MD5 algorithm is explored for key generation and key verification. After the key verification, the trusted measures such as reputation value, positive edge and negative edge values are computed to formulate the trusted network.

Keywords: Mobile Ad Hoc Network, Malicious Node, Cluster and Reputation Scheme

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

1. Introduction

The idea of implementation of mobile wireless devices working collectively was proposed in the 1990s, when significant amount of research activities were carried out on mobile ad hoc networks (MANETs). The MobileAd hoc Networks Working Group [1] was created in 1997, with the aim of standardizing routing protocols forMANETs. Two standard specifications for track routing protocol were developed by this group, namely the reactiveand proactive MANET protocols. Each node in a MANET is a computer acting as both a host and arouter, having the job of forwarding the packets between two nodes which are not in direct communication withone another. Each MANET node requires a much smaller frequency spectrum that a node requires in an affixedinfrastructure network [1].

A MANET is an autonomous collection of mobile user nodes communicating over wireless links, with a relative bandwidth constraint. Since the nodes are mobile, the network topology is more probable to unpredictablechanges over time. A MANET is usually decentralized, *i.e.* all network activities including topology determinationand message delivery, should be executed by the individual nodes themselves. Therefore, the routing functionalitygets incorporated into the mobile nodes. **Figure 1** illustrates the infrastructure of nodes in MANET [2].

Mobile Ad hoc Network got outstanding success as well as tremendous attention due to certain characteristics such as self-maintenance and self-configuration. At early stages, researchers focused mostly on its user-friendlyand mutual environment, however, many different problems came into being; security is one of the major issuessince providing secure communication between different nodes in a mobile ad hoc network environment hasbecome difficult. Finally, MANETs can be considered as an infrastructure less, multi-hop network with mostimportantly its self-organizing property [3] [4]. Due to its wireless and distributed environment, the system securitybecomes a challenging task for the designers. In the last few years, security problems in MANETs haveattracted much attention, thereby making the researchers to focus on specific security

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

areas, like intrusion detectionand response, establishment of trust infrastructure and securing routing protocols.

Intrusion detection (ID) [5] [6] in MANETs is more complex and challenging than in fixed networks, because of the difficulty in collecting the audit data from the network, and applying ID techniques in detecting intrusions at alow rate of false positives and an effective response to intrusion. Certain features of MANETs create implementationand operational complexities, and such additional challenges for ID schemes in MANETs are as follows [7] [8] [9] [10] [11]:

- Lack of concentration points during audit data collection and monitoring.
- The routing protocols in MANET necessitate cooperation of nodes to act as routers, thereby creating opportunity for attacks.
- Dynamic and unpredictable network topology due to mobility of nodes, making the process of intrusion detection complicated.
- Complex ID schemes due to the limited computational ability of most of the nodes.

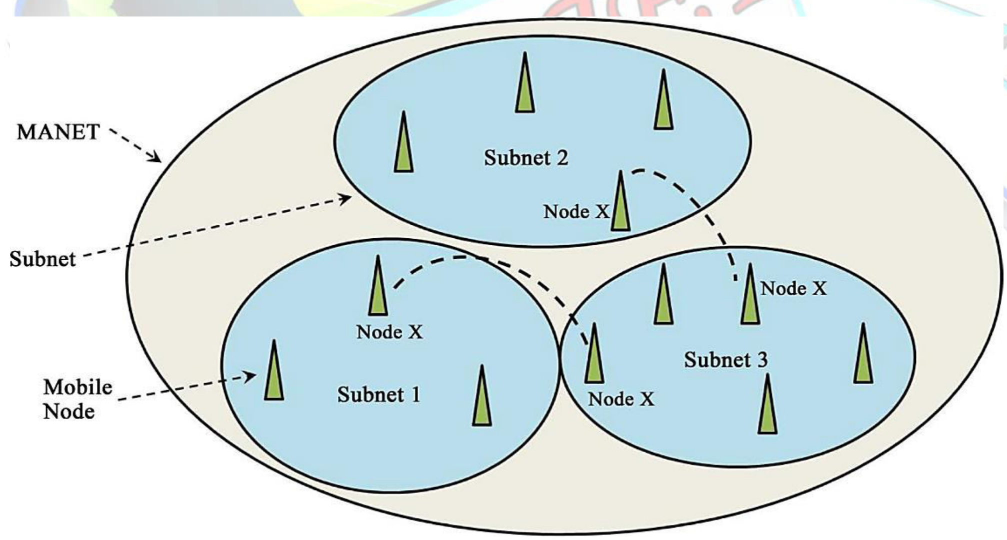

Figure 1: Interfacing modes in MANET

2. Reputation based Aware Key Generation (RAKG)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Privacy, authentication and access control are the essential features that should be present. These features are vital in the case of any wireless networks than the wired network communications due to the widely shared nature of the wireless medium. Themain objective of this paper is to provide a cosine similarity-based clustering and dynamic trustaware key generation model for efficiently validating the trust of the participants in the presenceof malicious behavior. To achieve this goal, this paper invented a similarity-based clusteringapproach and also introduces an improved MD5 algorithm. The overall working principle of theproposed approach is described in the following algorithm:

2.1 Clustering based on Cosine Similarity

The Euclidean distance between two nodes is calculated as follows:

$$d\ (m.n) = \sqrt{(m_1 - n_1)^2 + (m_2 - n_2)^2}$$

Based on the Euclidean distance, the nodes are calculated the trusted computation. The distance computation is used to find the shortest distance and the optimal path selection at the time ofnew connection establishment. The attributes taken for distance calculation are the port numberfor the corresponding node and the location information of that particular node.The similarity metric describes to what extent two or more agents/participants are alike. The similarity between the nodes is calculated based on the cosine similarity measure. Based on thissimilarity measure, the *k* clusters are formed. Each cluster includes a set of similar users.

Algorithm 1 Dynamic reputation trust aware key generation algorithm.

Input: Set of Nodes

Output: Trusted Network

Step 1: Network Setup

1: Deploy the network with ‘*n*’ nodes

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Step 2: Distance calculation

2: For each node *i* in network

3: Compute Euclidean distance $d(m \cdot n)$

Step 3: Clustering the nodes

4: For each node *i* in network N

5: Compute Cosine similarity *Similarity [i] [j]*

6: Cluster the similar characteristic nodes

Step 4: Key Generation

7: $Key = ip\_id \oplus c\_id$

Step 5: Key Verification

8: Verify the generated keys

Step 6: Neighbour Connection Request

9: Source node sendReq to Destination

10: Destination node send the Req-reply to the source node

Step 7: Formulate Trusted Network

11: Source node verifies the key and sends ack to Destination

12: **if** $TR > T$

13: establish communication

14: **else**

15: malicious node

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Cosine similarity measures the similarity between two vectors *A* and *B* of *n* dimensions. The cosine of two vectors is mathematically derived based on the Euclidean dot product formula. The proposed cosine similarity measure yields more accurate clustering results. For example, if the network includes *n* nodes, then each node has a unique ip_address (ip_id). The similarityvalue is estimated for each pair of nodes. The similarity values are arranged in an ascendingorder. The *k* clusters are predefined and nodes are grouped into disjoint clusters based on thesimilarity measure. Each cluster has a unique cluster_id (*c*_id), which is used to generate a keyvalue of node.

2.2 Key generation

In this section, the improved MD5 algorithm is discussed with the appropriate algorithm. After the nodes are clustered, the nodes can initiate communication with other nodes. Each node witha key value is generated based on the following MD5 algorithm. The key value includes thenode ip_address and their corresponding cluster_id. The MD5 algorithm can be used as a digitalsignature mechanism. It takes as input a message of arbitrary length and produces as outputa 128-bit fingerprint or message digest of the input. It is estimated that it is computationallyinfeasible to produce two messages having the same message digest. MD5 hashes are also usedto ensure the data integrity of files because the MD5 hash algorithm always produces the sameoutput for the same given input. Then, users can compare a hash of the source file with a newly created hash of the destination file to check that it is intact and unmodified.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

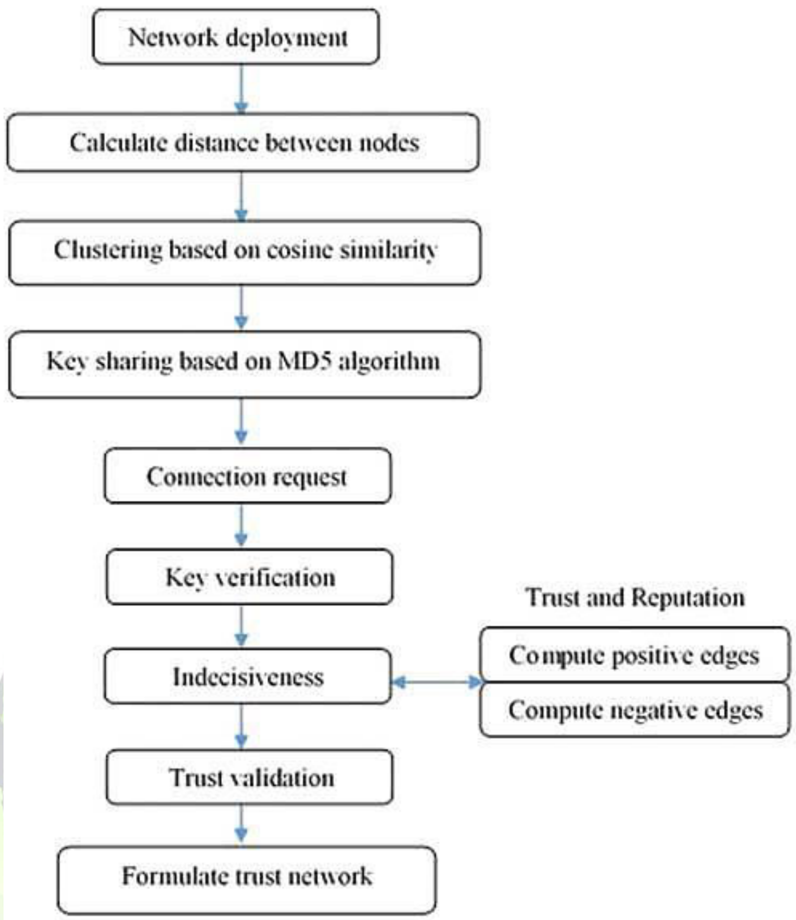

Figure 2: Structure of the proposed Cluster and Reputation trust aware key generation scheme

Algorithm 2 Cosine similarity of nodes.

Input: Node list (IP_List), Attributes of nodes (PropertiesList)

Output: Similarity between nodes

N←−IP_List.size();

For *I* = 1 to *n*nodes

Ip1←−IP_List.get(*I*)

Properties pros←−Ip1.getProperties()

V1 = Vector

For $J = 1, j$ <PropertiesList.size(), J++ do

If (Properties.contains(PropertiesList.get(J)) then

V1[i][j] = 1

Else

V1[i][j] = 0

End If

End For

End For

For $J = 1$ to $n$attributes

Similarity [I] [J] = V [I] $*V$ [J]/mod ($V1$ [I]) $*$ mod ($V2$ [J])

End For

End For

Return Similarity

Algorithm 3 Improved MD5 algorithm for key generation and verification.

Input: Node ip (IP_list) and Cluster_id (Cid_list)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Output: List of key values of all node & verification

// Key generation steps

Step 1: For all nodes *n*

Step 2: Generate MD5 hash for node_ip for node *i*

Step 3: Generate MD5 hash for cluster_id in which node *i* exists

Step 4: Key = MD5_ ⊕ MD5_*cid*

//KeyVerification Mechanism

Step 5: Key verification of node *i*

Step 6: Retrieve the cluster id (cid) from server

Step 7: Retrieve the generated keys from server (key1)

Step 8: Key 2 = MD5_ip ⊕ MD5_cid

Step 9: If key 1 = key 2

Step 10: Accept the node

Step 11: Else

Step 12: Mark it as a malicious node

Step 13: End

The list of node ip_address and the list of cluster_idis given as the input and the result will bethe generated key values of all the nodes. The existing MD5 algorithm generates a single key.The improved MD5 algorithm XORs the keys between the node ip and the cluster id. Hence, itprovides better trustworthiness in social networks. The above key verification algorithm checkswhether the two participants are sharing the same key or not. If it shares the same key, then thatnode will be accepted or it will be rejected,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

because it is obviously known as a malicious node.Figure 3 depicts the generated key value for the individual node IP with the corresponding clusterID.

Cluster ID	Node Ip	KeyValue
1	194.027.251.021	9E23E19ACFC6F472B5BA58...
1	172.016.118.070	66DBE6A673416E5E965573F...
1	207.230.054.203	E4AF5595267CD5B8E44126...
2	135.008.060.182	79D38708B26E5F38FE8D51...
2	172.016.113.204	2F915E2D3E3F78DDF377A7...
2	172.016.112.100	4F93C2321930BDB07F3D06...
3	206.048.044.018	EBFF69C849A88FA2793A1D7...
3	209.001.012.046	00C128BD5EFE0FB4F17080...
3	208.239.005.230	9240462E8723D567CE562C...
4	153.107.252.061	A9032CAFDAB116BB37D40B...
4	153.107.022.061	77C0EE35D58935710B3FF1...
4	205.160.208.190	2D37E3813DACE4D5232771...
4	172.016.115.234	4E05BC621CA600234BC2FC...

Figure 4: Key Generation

2.3 Trust and Reputation Computation

Trust is a node belief in another node capabilities, reliability and honesty based on its direct experiences. Reputation is a node belief in another node capabilities, reliability and honesty based onrecommendations received from other nodes. Reputation can be consolidated/centralized, whichis computed by a trusted third party. Even though, trust and reputation are different, they areclosely related. Both are used to compute nodes' trustworthiness. The trust value between thetwo participants' nodes is estimated based on the following calculation:

$$Trust\ Value\ (existing) = \frac{Number\ of\ positive}{Overall\ items} \quad (2)$$

Based on Equation (2), the existing trust models computed the trust value. They do not considerthe negative computation values. The proposed trust computation model takes the positivecomputation as well as the negative computation. The positive, negative and trust computationsare described in the following equations:

$$Positive\ computation = e^{-\alpha/n} \quad (3)$$

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

$$Negative\ computation = e^{-\beta/n} \qquad (4)$$

$$TR = \frac{(e^{-\alpha/n} + e^{-\beta/n} + rep)}{3} \qquad (5)$$

Here, positive computation leads to an increase in trust, that is, above the threshold value and negative computation leads to the decrease in trust, that is, below the threshold value, α denotesthe number of equal terms, β denotes the number of unequal terms and n denotes the overallitems. Reputation occurred means that value results in '1'; otherwise, results in '0'. Rep denotesthe reputation value, that is, the number of repeated values. Based on the trust calculation, thethreshold value T is fixed. Threshold is the mean value for all data present in the similaritymatrix.

$$T = \frac{sum\ of\ values\ in\ positive\ and\ negative\ matrix}{number\ of\ rows * number\ of\ columns} \qquad (6)$$

If the trust value TR > T, then it is a trusted node. Else, it is declared as a malicious node. TR denotes the trust rate. The attributes for the computation of the trust value is taken from thecommunication information such as source byte, source address and destination address.Trust of each node is computed based on the following properties such as source bytes, receivedbytes, request and communication node. The trusted network is formulated based on the trustand reputation computation.

3. Implementation Result and Discussion

The proposed Clustering and Reputation Scheme (CR) compared with the Reputation Trust Model (RTM) is compared. The network nodes are divided into diverse clustersbased on the cosine similarity measure. Each node has a unique id and each cluster is labeled with a unique id. The node ids and the cluster ids are used to generate the key based on animproved MD5 algorithm. The DARPA IDS evaluation data-set has been taken and deliberatedby many as a very outmoded data-set, and moreover, it cannot accommodate the latest trend inattacks. The DARPA IDS data-set is used to train and test the performance of Intrusion DetectionSystem. In the DARPA IDS data-set, all the network traffic comprising with the complete payloadof each packet is noted in tcpdump

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

format and delivered for evaluation.To validate the performance of the proposed framework, the following metrics are taken:accuracy, key strength, trust value and success ratio (SR).

$$Accuracy\ Analysis = \frac{Sum\ of\ all\ positive\ edges}{Total\ number\ of\ edges} \quad (7)$$

$$Success\ Ratio = \frac{\sum_{i=0}^{N} S_i}{\sum_{i=0}^{N} O_i} \quad (8)$$

where SR denotes the success ratio, *Si* denotes the successful connections and *Oi*denotes theoverall connections.

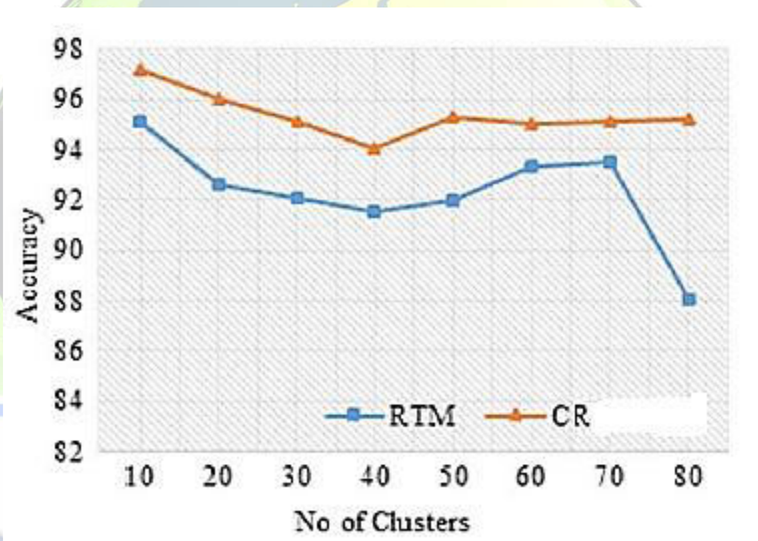

Figure 5: Performance analysis of the proposed CR and Existing RTM on Accuracy

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

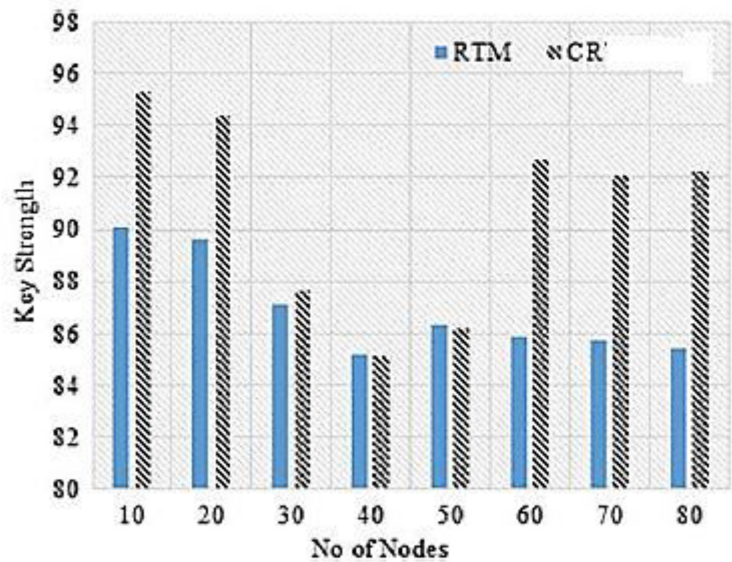

Figure 6: Performance analysis on Key Strength using proposed CR and RTM

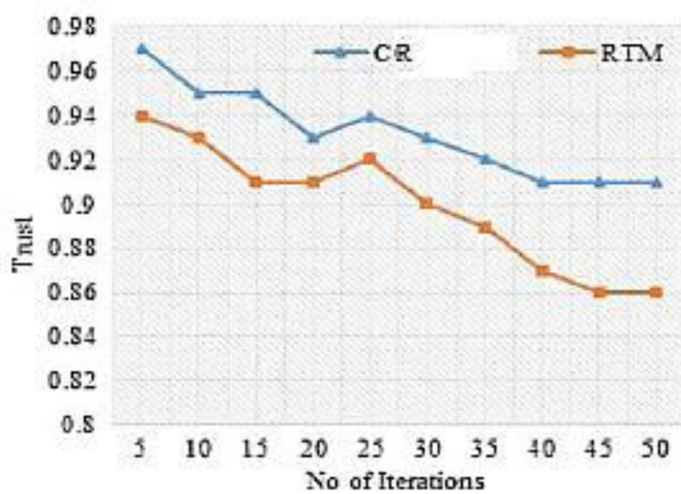

Figure 7: Trust between the proposed CR and RTM based on number of iterations

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

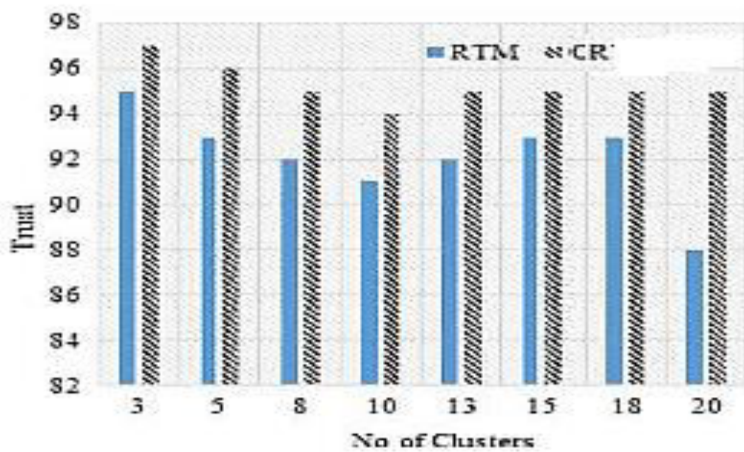

Figure 8: Trust between the proposed CR and RTM based on number of clusters

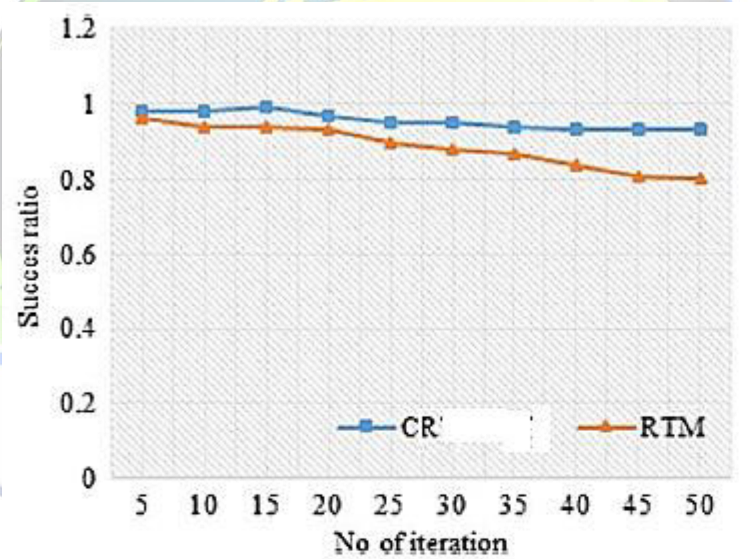

Figure 9: Performance analysis on Success ration of proposed CR and RTM based on number of iterations

4. Conclusion

A novel CR scheme is proposed and implemented. The proposed structure utilizes the cosine similarity measure for clustering the network nodes. Also, the Euclidean distance is estimatedfor trust node participation. An improved MD5 algorithm is explored for key generationand key verification. The trusted network is formulated for trusted communication with the correspondingusers. The experimental results show that the proposed system can perform betterthan the existing. In the future, several security algorithms and techniques will be analysed and incorporated the best resulting security algorithm with this framework in order to provide the high-level securecommunication for source–destination packet transmission.

Reference

[1] Zeng, Y.Q., Chen, Z.D., Qiao, C. and Xu, L. (2011) A Cluster Header Election Scheme Based on Auction Mechanismfor Intrusion Detection in MANET. *International Conference on Network Computing and Information Security*,433-437.

[2] Chang, J.-M., Tsou, P.-C., Woungang, I., Chao, H.-C. and Lai, C.-F. (2015) Defending against Collaborative Attacksby Malicious Nodes in MANETs: Cooperative Bait Detection Approach. *IEEE Systems Journal*, **9**, 619-621.

[3] Adnan, A., Kamalrulnizam, A., Muhammad Ibrahim, C., Khalid, H. and Abdul Waheed, K. (2014) A Survey on TrustBased Detection and Isolation of Malicious Nodes in Ad-Hoc and Sensor Networks. Frontiers of Computer Science,Higher Education Press and Springer-Verlag Berlin Heidelberg.

[4] Chakraborty, S., Nandi, S. and Chattopadhyay, S. (2016) Alleviating Hidden and Exposed Nodes in High-ThroughputWireless Mesh Networks. *IEEE Transactions on Wireless Communications*, **15**, 928-937.http://dx.doi.org/10.1109/TWC.2015.2480398.

[5] Tselikis, C., Mitropoulos, S., Komninos, N. and Douligeris, C. (2012) Degree-Based Clustering Algorithms for WirelessAd Hoc Networks Under Attack. *IEEE Communications Letters*, **16**, 619-621.http://dx.doi.org/10.1109/LCOMM.2012.031912.112484.

[6] Karunakaran, S. and Thangaraj, P. (2011) A Cluster-Based Service Discovery Protocol for Mobile Ad-hoc Networks.*American Journal of Scientific Research*, **11**, 179-190.

[7] Su, Y.Y., Hwang, S.F. and Dow, C.R. (2008) An Efficient Cluster-Based Routing Algorithm in Ad Hoc Networks withUnidirectional Links. *Journal of Information Science and Engineering*, **24**, 1409-1428.

[8] Han, B. and Jia, W.J. (2007) Clustering Wireless Ad Hoc Networks with Weakly Connected Dominating Set. *Journalof Parallel and Distributed Computing*, **67**, 727-737. http://dx.doi.org/10.1016/j.jpdc.2007.03.001.

[9] Cheng, C.-T., Tse, C.K. and Lau, F.C.M. (2011) A Clustering Algorithm for Wireless Sensor Networks Based on Social Insect Colonies. IEEE Sensors Journal, 11, 711-721. http://dx.doi.org/10.1109/JSEN.2010.2063021.

[10] Fatima Zohra, M., MaazaZoulikha, M. and Said, K. (2011) Techniques of Detection of the Hidden Node in Wireless Ad Hoc Network.*Proceedings of the World Congress on Engineering*, **2**, 978-988.

[11] Abusubaih, M. (2011) A Combined Approach for Detecting Hidden Nodes in 802.11 Wireless LANs. Annals of Telecommunications.*Annales des Telecommunications*, **66**, 635-642.