Attack Resistance Dynamic Detection and Data Trust Routing in MANET

Syeda Kausar Fatima
Research Scholar, JNTUH, India

Syed Abdul Sattar, PhD
Prof & Dean SAKCET, TS, India

D. Srinivasa Rao, PhD
Prof. ECE Dept. JNTUH, India

ABSTRACT

Organizing trust in Ad Hoc network is a challenging task when environment cooperation is critical to achieving system goals such as reliability and scalability. Ad Hoc networks are easily accessible due to its dynamic nature. The main issue is to assure secure network services. In order to achieve this, a secure organizing trust aware routing is always research challenge in Mobile Adhoc Networks. This paper organizes the trust level to improve trust organization system in MANET by achieving attack resistance. To achieve attack resistance level, we contribute our research by understanding trust factors in MANET. This paper has been prepared keeping in mind that it needs to prove itself to be a valued resource dealing with both the important core and the focused security issues in this area.

Keywords

MANET, Security, Trust Management in MANET

1. INTRODUCTION

MANETs are self-sufficient systems consisting of mobile nodes that are linked by multi-hop wireless links. Trust Model which are established for wired network cannot be used in wireless network. MANETs are highly susceptible to various security attacks. Providing secure Communication in MANET is proved to be a important challenge. Common validation schemes are not applicable in Ad hoc network since public key infrastructure is hard to deploy [1] [2].

In mobile ad hoc networks (MANETs), the scattered decision making should take into account trust in the elements: the sources of evidence, the processors of information, the fundamentals of the communications network across which the evidence is communicated, etc.[3] This trust must often be derived under time-critical conditions, and in a distributed way. In MANETs, reputation-based trust management systems are shown to be an actual way to cope with adversary.[4] By launching trust with the nodes it has or has not directly related, a node in the network diagnoses other nodes and predicts their future behaviour in the network. Hence, trust plays a key role for a node in selecting with which nodes it should cooperate, refining data availability in the network. Further, scrutinizing trust values has been shown to lead to the detection of malicious nodes in MANETs. Despite all the growth for securing MANETs, leads to added challenges. Trust organization mechanism is considered to be an effective dimension to solve these problems [4]. In the situation of MANET, there are several trust management models that have been proposed in the realm of network [5], where trust can be considered as the reliance of a network node on the ability to forward packets or offer services timely, integrally and reliably. In the existing models, decision factors are often incomplete in the trust derivation, which are not fully integrated with the inherent characteristics of MANET. When the factors of decision-making are given, though we know that different factors have different weights, the precise weights are difficult to determine. Existing methods in these models for weight determination are lack of rationality and practicability. As a result, they cannot calculate an accurate trust value for each node. Hence, these models are ineffective in MANET trust management, and their applications are very simple [5].

1.1 Motivation for Trust Management in MANETs

The concept of “Trust” initially derives from social sciences and is well-defined as the degree of particular certainty about the behaviours of a specific entity [7]. Blaze et al. [8] first introduced the term ”Trust Management” and recognised it as a discrete factor of security service area in networks and explained that ”Trust organization provides a unified approach for specifying and understanding security policies, credentials, and relationships.” Trust management in MANETs is needed when participating nodes, without any previous connections, desire to found a network with an satisfactory level of trust relationships among themselves. Examples would be in building initial trust bootstrapping [9], combination operations without predefined trust, and validation of certificates generated by another party when links are down or ensuring safety before entering a new zone [10]. In addition, trust management has varied applicability in many decision making circumstances including intrusion detection, authentication, access control, key management, segregating misbehaving nodes for effective routing, and other purposes. Trust management, including trust establishment, trust update, and trust revocation, in MANETs is also much more challenging than in traditional centralized environments. For example, collecting trust information or suggestion to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often restrict only the trust assessment process.

2. RELATED WORK

Govindan and Prasant et al [8] considered trust propagation, aggregation and prediction as the main trust dynamics which can help in trust computations. According to them the trust computation is based on following metrics Trust propagation • Trust aggregation • Trust prediction • Trust applications. The trust values will be propagated in the network so that the trust can be established between nodes which are not in immediate contact. While propagating the trust, trust values from multiple paths will be aggregated to get a combined trust value which can be stored in the history. The stored trust value will be used in the trust predictions and this predicted trust value will be further used in the applications that need security. The stored trust value can also be used in the trust computation block in the form of feedback knowledge. Therefore, trust computations, trust propagation, trust aggregation and trust prediction blocks are closely interconnected in our envisioned trust system but the system computes extract computational resources to organize trust in MANET and the trust prediction is not accurate.

In the ATM scheme [9] there are two major functional modules: behavior data collection and trust management. The trustworthiness of each node is then assessed in the trust management module. In the ATM scheme, we train and then use a SVM classifier to evaluate the trustworthiness of the nodes. The trust management module supports the following two modes for the SVM classifier: training mode and testing mode. In the training mode, several known adversaries exhibiting known misbehaviours are deployed in the network to generate the training dataset so that a SVM classifier can be learned from this dataset.

In [10], proposes a fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust. Instead of using hard security approaches, as in traditional security techniques, to eliminate security vulnerabilities, our work aims to maximize performance by trading off risk (i.e., security vulnerability) for trust. In this work, we propose a composite trust-based public key management (CTPKM) with no centralized trust entity with the goal of maximizing performance (e.g., service availability or efficiency) while mitigating security vulnerability. Each node employs a trust threshold to determine whether or not to trust another node. Each node's decision making using the given trust threshold affects performance and security of CTPKM

In [11], classify the clustering scheme for trust-based clustering schemes and illustrate how reputations are integrated in these schemes. Trust-based clustering algorithms integrate the trust management systems with clustering algorithms to decrease the overheads of reputation management. The growing interest in the reputation-based systems inspired numerous trust-based clustering schemes for MANETs. But there is a lack of solution to operate in both secure and hostile environments.

Raihana Ferdous et al [12] have proposed a Cluster head(s) selection algorithm based on an efficient trust model. This algorithm aims to elect trustworthy stable cluster head(s) that can provide secure communication via cooperative nodes. However the way the messages passed through may overload the Cluster head, creating a bottleneck due to additional message exchanges. Another possible limitation is the way that the message authentication between intermediate Cluster heads are treated, where there can be a delay in identifying a malicious neighboring node.

Li et al. [13] classify trust management as reputation-based framework and trust establishment framework. A reputation based framework uses direct observation and second-hand information distributed among a network to evaluate other nodes. A trust establishment framework evaluates neighbouring nodes based on direct observations while trust relations between two nodes with no prior direct interactions are built through a combination of opinions from intermediate nodes.

Yuxin Liu et al. [14] proposed active trust that avoids black holes through active creation of number of detection rotes to quickly detect and obtain nodal trust and improve data route security. This scheme detects the misbehavior but it does not isolate it. Therefore, in our system, we are considering only those nodes which are isolated by rating their trust value as low as 0 for non-cooperation.

3. PROBLEM DEFNITION

In this section, the research problem that is addressed will be defined in more detail, comprising the network model as well as the adversary model.

A. Network Model

A Mobile Adhoc Network generally refers to a wireless network of heterogeneous nodes or other computing devicesresponsible for dynamically discovering other nodes for forwarding packets to their destination.This type of network enables continuous monitoring of mobile nodes and secure data transmission. All of the nodes in MANETs are equipped with the same wireless communication interface, such as IEEE 802.11g. The nodes are limited in energy as well as computational and storage capabilities.

B. Adversary Model

First of all, the nodes are assumed to be trustworthy since they are usually better protected. The connected mobile nodes, are generally more susceptible to various attacks, and they can be compromised at any time after the MANET is formed. The adversary can be an outsider located in the wireless range of the mobile nodes, or the adversary can first compromise one or more nodes and behave as an insider later. The adversary is able to eavesdrop, jam, modify, forge, or drop the wireless communication between any devices in range. The goals of the adversary may include intercepting the normal data transmission, forging or modifying data, framing the benign devices by deliberately submitting fake recommendations. More specifically, malicious attacks are considered in this paper.

C. Cluster Formation

After deployment of nodes into network, the nodes broadcast packet P_i which it represents initial trust value (T_i), node id (N_i) , and node coordinates (N_{x_i}, N_{y_i}). Cluster formation function represents all these values $f(C_i) = \{N_i, P_i, T_i\}$. The network area is divided into different zones $(x) = \begin{cases} \log_x X\,, \\ \log_x Y\,,\ x \geq 1 \end{cases}$, where x represent number of zones. Each zone again sub-portioned into horizontal level. The nodes are divided with corresponding zone function, based on the cluster function the nodes are initialized into the cluster. A circle is formed with a fixed radius by selecting (either randomly or with highest cooperating neighbor density within 1 hop distance) a node as center and an arbitrary small length as radius. Center of the new circle is computed as the mean of the points within the circle while the radius in increased by the distance of two successive centers. The nodes reply back and in this way clusters are formed in the network.

4. PROPOSED MODEL

The main goal is to convince the adversary to launch an attack where the system can identify the attack behavior and then isolate the attacker. Thus, the proposed system can lower the trust of suspicious nodes and increases the node trust in network routing. In attack resistance detection routing, nodal trust can be easily identified and it can easily identify the trusted routes by choosing trusted nodes by resisting the route against black holes.

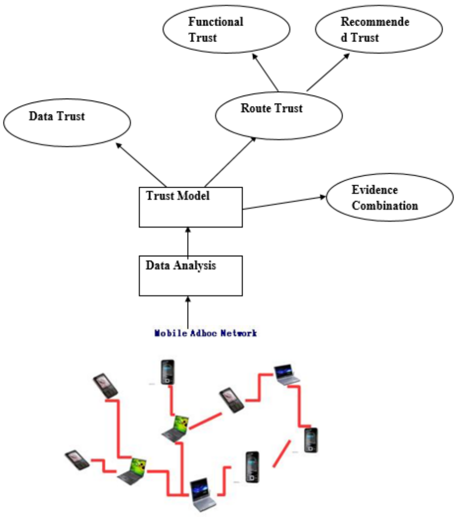

Fig 1: Proposed Model Block Diagram

4.1 Classification of Trust Types

There are three different trust types such as Route trust, Data trust and Evidence Combination trust are considered in proposed model.

Route Trust or Path Trust

The route trust expresses the credibility for the set of nodes on a routing path, and its value is defined as the minimum of one-hop trust values. The source nodes determine service level basing on the assessment of route trust value. The route trust value can be defined as a constraint in the trusted routing decision making.

$$\text{Route Trust: } RT_{sd} = \min_{\substack{s \le n \le d-1 \\ k = n+1}} \{TV_{nk}\} \qquad (1)$$

To calculate route trust, the RREQ and RREP packets are modified so that they contain the trust value of the node from which the packet is received. Both packets are changed because during route discovery a node transmits the RREQ packet by broadcasting [5]. A node knows only the node from which the packet is received, not the node to which it is to be transmitted. Therefore, the RREQ packet is modified to incorporate the previous node's trust value and the RREP packet is modified to incorporate the next node's trust value.

Algorithm 1: Attack Resistance Dynamic Detection Routing:

```
Initiate Route Request $RREQ$
For :
    Discover neighbour node for each node $N_i$:
    Let $N_i$.accesTime=Current_time
End for
For: each node which produces a detection packet $P$, such as node $N$ , Do
    Create packet $p$, and do value assignment for $\alpha$ and $\alpha'$
    Choose node M as the next hop which node M meets access time is the minimum and nearer the sink
    Send packet $p$ to node M
End for
For each node that receives a detection packet, such as node M, Do
    let P. $\alpha$ =P. $\alpha$ -1, P. $\alpha'$ =P. $\alpha'$ -1
    If P. $\alpha'$ =0 then
        Build opinion packet q, and make value assignment for each part
        Send opinion packet q to the source
    End if
    If  0 then P. $\alpha$ $\neq$ 17: detection routing continue
    End if
End for
For each node that receives opinion packet q, such as node $L$, Do
    If q.destination is not itself then
        send q to the source node
    End if
End for
```

The attack resistance dynamic detection routing protocol packet structure represented into six different parts. (1) packet head (2) packet type (3) Source node ID (4) Max detection route length (5) Source node sends packet acknowledge for every hops (6) Packet ID

Table1: Detection Routes Packet Structure

Phead	Ptype	SID	α	α'	PID

According to the figure, the source node selects neighbour node to launch the detection route. When the node receives a detection packet from source node the route length α is decreased by 1. Then after that the max detection route length α become a 0, to generate a route trace packet and produce a route trace to the source and the restores α to the initial value. If the α is 0 then selects next route o hop to in similar manner. The structure of reverse trace packet is composed of following parameters 1) packet head (2) packet type (3) Source node ID (4) destination id (5) detection packet id (6) Packet ID

Table2: Reverse Trace Packet

Phead	Ptype	SID	DID	τ	PID

The route trace packet routed backed to the source node with destination node information. The route track packet process is clearly presented in Algorithm-1.

4.2 Route Trust Calculation

While detection routing and data routing, each node performs a nodal trust calculation to assist in routing level attack avoidance. If node A performs a routing for node B at time t, if the data detection are successfully routed, then consider the trust of node from A to B to be $\Delta_A^B(t)$ otherwise consider trust value as $\Lambda_A^B(t)$

Let consider node A interacts with node B within a time span of t, the detection value of the node A is determined as follows

$$\{\Delta_A^B(t_1)\big|\wedge_A^B(t_1), \Delta_A^B(t_2)\big|\wedge_A^B(t_2), \ldots . \Delta_A^B(t_{n-1})|\wedge_A^B(t_{n-1})\}$$
(2)

$\Delta_A^B(t_i)|\wedge_A^B(t_i)$ represents a trust value between node A to B at time $t_i$is a trust. The detection routing scheme estimates the trust value at following levels i.e direct trust, recommended trust and compressive trust. The direct trust value between node A to B is measured as

Let consider the trust set of node A to B at time span t_i. The direct trust of node A to B as

$$DT_A^B = \sum_{i=1}^{n} \{(\Delta_A^B(t_{n-1})\big| \wedge_A^B (t_{n-1})). af(i)\} /w \qquad (3)$$

Where $af(i)$ is an attenuation function to weight direction trusts at different times [0,1]. In this scheme, the trust calculation should meet the following condition. If the node is found to be malicious in the latest detection, then its trust should be below the threshold, and the node will not be chosen for later routing. If the malicious node returns to the normal node, it needs several detections to take it into routing consideration.

In recommended trust, the Node A is the trust evaluator, node E is the target of evaluation, and node B is a recommender of A. Consider E_A^B to be the direction trust of A to B andE_B^C to be the direction trust of B to C; then, the recommendation trust of A to C is

$$RT_A^C = E_A^B + E_B^C \qquad (4)$$

Comprehensive trust is the total trust, which merges the recommendation trust and direction trust:

$$CT_{A,B}^T = \alpha E_A^B + (1-\alpha) E_B^C \qquad (5)$$

Once the node initiates a detection route, it estimates the direction trust according to direct trust Eq. (3) for received feedback packet. Through interactions, the node obtains the recommendation trust from its neighbors according to recommended trust Eq. (4). Finally, it calculates the comprehensive trust according to Eq. (5).

4.3 Data Trust

The main idea of this trust type is to determine trustworthiness of traffic data (data trust) is evaluated based on the data sensed and collected from multiple mobile nodes. We propose the use of the semantics of the data, and correlate it with observations from neighbour [3] nodes. The data transmission is occurred based on trust values and discovers shortest path distance. If source and destination are presented within same region, checks teh trust value of each other and invokes direct communication. If it is indirect communication, a forwarder node discovers nearest node to the sink node from set of candidates whose trust is greater than preset threshold as the next hop. If the forwarder node cannot locate any such suitable next hop node, it will send an opinion failure to the sender node, and the sender node will re-calculate the unselected node set and select the node with the largest trust as the next hop; similarly, if it cannot find any such appropriate next hop, it sends a feedback failure to its sender node. This process should repeat until it identifies an appropriate next hop node. Once sender nodes obtains secured connection the secured data transmission takes place, which is presented in next section.

Algorithm 2: Data Trust Calculation:

```
1 For each node that produces or receives a data packet, such as node $N$, Do
2: select a next hop node $M$ where the node $M$ has higher trust, near to destination $D$ and never been selected in this data routing process
4: If $N$ discovers such node $M$, for that instance,
5: Encrypt the data packet P sent to node $M$
6: If node $M$ is the destination then
7: check the trust level $D_{tl}$ where $D_{tl} == DT_A^B$, then encrypt the data send to the destination
8: End if
9 :  Else
10: Send failure opinion to the upper node, such as node $L$
11: End if
12: End for
13: For each node that receives failure opinion, such as node $M$, Do
14: Repeat step 2 to step 11
15: End for
```

4.4 Evidence Combination Trust

In AdHoc networks, nodes produces different amount of data, ensuring of the data is trusted or not is more critical factor. Generally data is collected as a pieces, it is essential to identity that whether the data is from the trusted source, and trust route. In order to ensure the trust combinations, the proposed scheme uses Dempster–Shafer Theory of Evidence (DST) [38] is used to combine together various piece of evidences even if some of them might not be accurate. In DST, probability is replaced by an uncertainty interval bounded by belief (*bel*) and plausibility (*pls*). Belief is the lower bound of this interval and represents supporting evidence. Plausibility is the upper bound of the interval and represents non-refuting evidence.

Let assume if a node N_a examines that one of its neighbour $N_b$packets with probability k, then the actual node N_a has $k$degree of belief for that particular packet droping of that nodeN_b and 0 degree of belief when that node N_b is absence. The belief value is measured with respective of event e_i at which is observer by node $N_a$is computed as

$$bel_{N_a}(e_i) = \sum_{j:e_j \in e_i} d_{N_a} e_j$$

Where $e_j$are all basic events, these basic events composes a main event as e_i. $d_{N_a} e_j$ is a view of the event e_j by a node N_a. According to the above formula, the node N_a gets a single event report e_j of node N_b . We can future derive the belief and Plausibility for the packet dropping level of node N_b by the following: $bel_{N_a} N_b = d_{N_a}(N_b) = k$ and plausibility $pls_{N_a} = 1 - bel_{N_a} N_b = 1 - k$. we define the combined packet dropping level of node $N_b$as the following

$$pd\, N_b = bel\,(N_b) = m(N_b) = \sum_{p=1}^{K} d_{N_a}(N_b)$$

Here $d_{N_a}(N_b)$ indicates the view of node N_a on another node N_b . We can combine reports from different nodes by applying the Dempster’s rule, which is defined as following

$$m_1 N_b \oplus m_2 N_b = \frac{\sum_{q,r:e_q \cap e_r = N_b} m_1(e_q) m_2(e_r)}{1 - \sum_{q,r:e_q \cap e_r = \Phi} m_1(e_q) m_2(e_r)}$$

Here we use DST to combine the local evidence collected by a node N_a itself and external evidence shared by other nodes.

5. TRUST EVALUATION

There are different assumptions considered to determine node trust. The active detection routing initiates detection route, initially each node initiates single detection route packet with certain route length (i.e The route length is number of hops and route length should vary with respective of network size). If the detection route length is α hops and one detection opinion packet is returned to the detection source every α ($\alpha \leq \bar{\alpha}$) hops, then the total number of detection hops in this route is

$$hop_{\bar{\alpha},\alpha} = \sum_{j=1}^{n} j\alpha + 2\bar{\alpha}$$

Active trust scheme can quickly detect malicious nodes based on successful routing probability, first ART calculates the success rate of any node in 1-hop transmission, if a failure node transmission means that sender node identifies that all of the detected nodes whose hops lesser than itself are black holes; the detected nodes cannot be selected, and sender node must select from the undetected nodes. If the selected undetected node is a black hole, the transmission fails. There are 3 states for sender node, that is, nodes whose hops are larger than, the same as and smaller than sender node's. For the nodal degree d, the number of nodes whose hops are smaller than sender node's is$d/3$, if direct trust node $m_d \geq d$, then all of the neighbours of sender node can be detected; then, only if all of the next hop nodes are black hole nodes the data transmission fail, the sender node broadcast this information to other nodes to avoid blackhole nodes for future communication. Then the sender node selects trusted nodes with average route length and distribute a data to destination.

6. SECURED COMMUNICATION AND DATA DISTRIBUTION

This section presents a secured data communication across mobile nodes, with dynamic detection routing and data trust management. Based on Attack Resistance Dynamic Detection Routing and Data trust routing algorithms, the source node S_i broadcast detection packet. The detection packet of source node contains the different route hops, where the detection packet interacts with group of mobile nodes, to obtain the detection status. In next stage the route trace packet, obtains the node route information with opinion of different hop nodes with help of opinion packets, which determines the node trust, once the data trust determines the node trust. The following process determines secured data communication.

Step 1: The sender generates a cluster key (C_{gk}) for group of nodes in a cluster C_i, after collecting the opinion of D_{tl} through detection hops $hop_{\bar{\alpha},\alpha}$. It generates a cluster key for different clusters C_i where $i = \{1,2, \dots \dots n\}$

Step 2: Then, the Source nodes multicast cluster key value in an encrypted form as $N_{ck} = C_{gk} \times hop_{\bar{\alpha},\alpha}$. The cluster members can find their cluster key using their secret key values as used $N_{ck} \; mod \; S_{ck} = C_{gk}$. The sender encrypts destination key and broadcast encrypted destination node key to the group of members in a discovered hops.

Step 3: Sender encrypts the data with encrypted cluster key N_{ck} to the next hop member, before broadcasting data to the next hop, the sender broadcast detection packet, where the opinion packet obtains node trust, based on node data trust condition the broadcast will exchange, if not it will not allow the node in the current hop, it will discover new hop where it can obtains suitable trusted nodes.

Step 4: After receiving the data from sender node, the forwarder node in a hop verifies the group key and cluster key to ensure source node.

Step 5: The forwarder node verifies the authentication of other hop nodes by processing group member key, $N_{chk} = C_{gk} \times hop_{\bar{\alpha},\alpha}$.

Step 6: Once the receiver receives a data from group of nodes, the receiver node decrypts the data which was forwarded by the nearest hop node using group key and verifies the authenticity of forwarder node.

$$D_R = (E_{ck} \&\& |N_{chk}| \&\& N_{ck}) == True$$

Step 7: The forwarder nodes can in turn forward the received data packet to other forwarder nodes by encrypting it using over a N_{chk} long range using multihop communication.

Step 8. After receiving the packets, the forward users can decrypt the packet using the D_R and process the messages.

7. EXPERIMENTAL STUDY

In this section, the performance of the proposed ARDDT approach is compared with the existing trust based routing mechanism of TEDR in MANET. The metrics used for the performance evaluation of the proposed ARDDT approach and existing approaches are PDR, throughput, average delay and detection rates. The proposed system is simulated with the network simulator-2 (NS-2) with the simulation parameters of Table 1.

Table 3: Simulation Parameters

No. of Nodes	50,100,150 and 200.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	20 sec
Traffic Source	CBR
Packet Size	512
Receiving Power	0.395
Sending power	0.660
Idle Power	0.035
Initial Energy	10.0 J
Attacks	Blackhole, Flooding Attacks
Data rate	2 Mbps

Packet delivery ratio – data packets successfully delivered to the destination / data packets generated by the source.

End-to-End Delay – the total time consumed that the data packet takes to reach from the source to destination vice versa.

Energy Consumption - It is the amount of energy consumed by the nodes for the data transmission.

Throughput – the average number of data packets transmitted per unit of time.

7.1. Simulation Results

The performance of ARDDT protocol is analyzed and the observations are made with respect to the parameters of packet delivery ratio, End-to-End Delay, routing packet overhead and throughput. Below figures demonstrate the performance of ARDDT protocol and TEDR at different attacks.

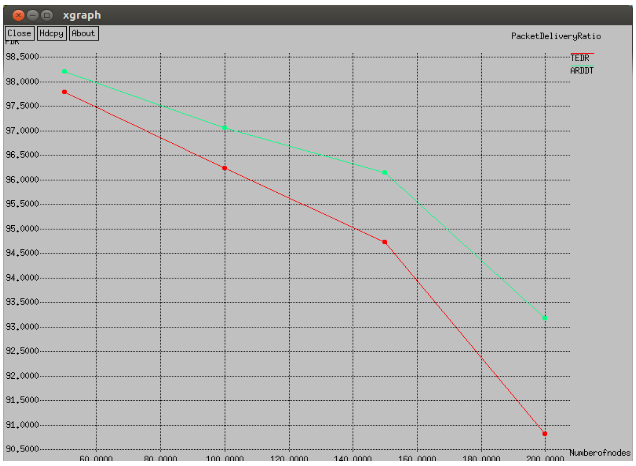

Fig 7.1 (a) Packet Delivery Ratio vs Nodes

According to Fig. 7.1 (a), ARDDT has the better packet delivery ratio than TEDR under different attacks. The packet delivery ratio of ARDDT protocol is around 97% and for TEDR is about 95% when there is no mobility. In case of TEDR, as the number of nodes increases the packet delivery ratio is decreased significantly about 7%. The biggest difference between ARDDT protocol and TEDR on packet delivery ratio is less than 8%.

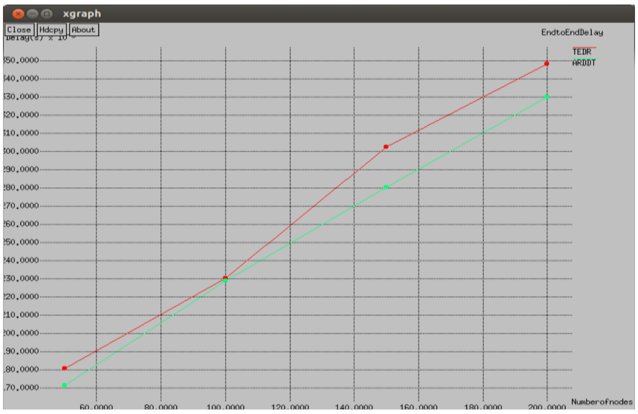

Fig 7.1 (b) End to End delay vs Speed

Fig. 7.1 (b) illustrates the end-to-end delay against different malicious nodes. According to the result, the delay rate increased with respective of number of nodes.

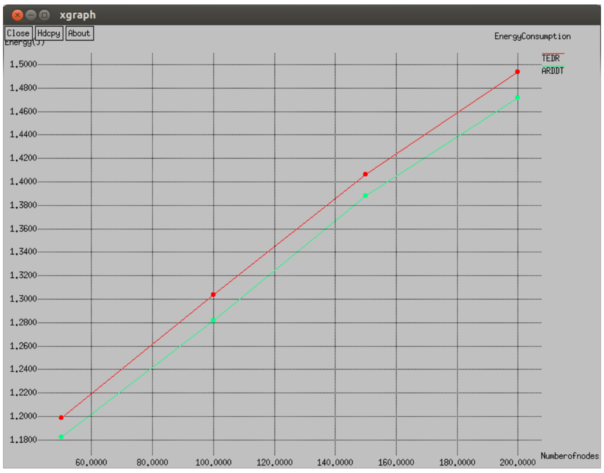

Fig 7.1 (c) Energy consumption vs Nodes

Fig. 7.1 (c) shows that the proposed ARDDT protocol and TEDR energy consumption performance with respective of number of nodes, where energy consumption rate increased with respective of attack level. Based on the results the energy consumption rate of ARDDT is lesser than TEDR.

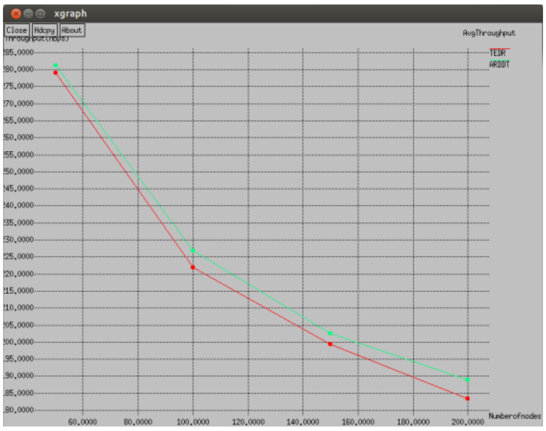

Fig 7.1 (d) Throughput vs Nodes

Fig. 7.1 (d) the average throughput rate of ARDDT is varied with respective of number of attacker nodes, where we estimated throughput rate by varying different malicious rate. The proposed model, ARDDT improved the reliability which it results to the better throughput compare to TEDR.

8. CONCLUSION

In this paper, Attack Resistance Dynamic Detection Routing and Data trust routing in MANET for resisting MANET against DoS attacks is carried. The proposed scheme determines the trust level at routing level, data level and evidence level. The trustworthiness of data and nodes are modelled and evaluated as two separate metrics, namely *data trust* and *node trust*, respectively. In particular, *data trust* is used to determine the node trust level before delivering data to the next hop node. This scheme predicts malicious on a traditional MANET by producing detection routing and data packets. In the next stage, secured data distribution is carried across different group of nodes in a cluster. The simulation results determines the efficiency of proposed routing protocol in comparison of existing TEDR protocol. According to the simulation results the ARDDT protocol manages attack nodes efficiently and produced better secured efficiency.

9. REFERENCES

[1] Heenavarshney and Pradeep Kumar, "Secure Communication Architecture Based On "BBCMS" Clustering Algorithm for Mobile Adhoc Network (MANET)", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-3, Issue-2, July 2013.

[2] Sandeep Kr. Agarwal, Amit Garg and K. V. Arya, "Security Issues & Clustering Based Solutions in Mobile Ad-hoc Networks - A Survey", Journal of International Academy of Physical Sciences, Vol. 16 No.3 (2012).

[3] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen. "A Survey on Trust Management for MobileAd Hoc Networks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2016.

[4] ErmanAyday and FaramarzFekri. "An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks", Georgia Institute of Technology, Atlanta, GA, 30332.

[5] Hui Xia1, Zhiping Jia1, Lei Ju1, Xin Li1, Youqin Zhu2. "A Subjective Trust Management Model with Multiple Decision Factors for MANET based on AHP and Fuzzy Logic Rules", IEEE/ACM International Conference on Green Computing and Communications, 2011.

[6] SînzianaMazilu*, MihaelaTeler*, CiprianDobre. "Securing Vehicular Networks based on Data-Trust Computation", Communications, 31(18), pp. 4343-4351, 2008.

[7] Poonam Gera, KumkumGarg, and Manoj Misra. "Trust-based Multi-Path Routing for Enhancing Data Security in MANETs", International Journal of Network Security, Vol.16, No.2, PP.102-111, Mar. 2014.

[8] Kannan Govindan and PrasantMohapatra. "Trust Computations and Trust Dynamics inMobile Adhoc Networks: A Survey", IEEE, 14(2), 279-298.

[9] Wenjia Li, Anupam Joshi and Tim Finin. "ATM: Automated Trust Management for Mobile Ad-hoc Networks Using Support Vector Machine", Baltimore, MD 21250.

[10] Jin-Hee Cho, Kevin S. Chan and Ing-Ray Chen. "Composite Trust-based Public Key Management in Mobile Ad Hoc Networks",IEEE 2014.

[11] MoazamBidaki and Mohammad Masdari. "Reputation-Based Clustering Algorithms in Mobile Ad Hoc Networks", International Journal of Advanced Science and Technology Vol. 54, May, 2013

[12] RaihanaFerdous, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan, "Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks", I Proceedings of IEEE INFOCOM, vol 4, Mar 2014, pp 2393-2403.

[13] J. Li, R. Li and J. Kato, Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks, IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[14] Yuxin Liu, Mianxiong Dong, Member, IEEE, Kaoru Ota, Member, IEEE, Anfeng Liu, "Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions 1556-6013 (c) 2016, pp. 1-14.

[15] Syeda Kausar Fatima, Dr.Syed Abdul Sattar, Dr. D. Srinivasa Rao and Syeda Gauhar Fatima " Trust Enhanced Dynamic Routing for MANET", International Journal of Advanced Research in Engineering and Technology Volume 8, Issue 3, May - June 2017, pp. 25–36.