Detection and Prevention of Black Hole Attack using Trust-TORA

N.Venkatadri[1] and K Ramesh Reddy[2]

[1] Research Scholar, Department of Computer Science, Vikrama Simhapuri University, Nellore.

[2] Assistant Professor, Department of Computer Science, Vikrama Simhapuri University, Nellore.

Abstract

Mobile Ad Hoc Network (MANET) is a collection of self configuring autonomous mobile nodes that communicate with one another through the use of wireless links. MANETs are infrastructure less networks, due to this characteristic, MANETs are used in various applications like battle fields, rescue operations, business applications, entertainment, education and so on. Nodes in MANET are communicated using insecure wireless channels due to this feature of MANET, they are very much prone to security threats.

Black Hole attack is a kind of DOS attack. The nodes which are affected by this attack are not transferred data packets to their neighboring nodes. Black hole nodes simply drop the packets whatever they received from their neighboring nodes. This attack severely affects the performance of the network.

In this work, we analyzed the impact of black hole attack and prevented the black hole attack by reputation based trust route mechanism. Previously lot of research has been carried out suing AODV and DSR. Many researches implemented various forms of DOS attacks and prevent these attacks by using different types of counter measures using AODV only. For this we used on-demand routing protocol TORA to detect and prevent black hole attack. Our proposed trust TORA performs well than original TORA under normal conditions and under harsh conditions. We measured the performance of network under normal conditions and under black hole attack using the performance metrics such as delay, packet delivery ratio and throughput.

Keywords

MANET, DOS Attacks, Simulation, Reputation based trust route mechanism, performance metrics.

1. Introduction

In recent years, MANETs have become more popular due to their features like inexpensive, easy to deploy under normal and harsh conditions while supporting high data rates [1]. VANETs are a specific type of the MANETs [10].Mobile ad hoc networks can be deployed very easily where no infrastructure exists and when it would be impractical to deploy infrastructure such as in rescue operations. Nodes in MANET can join or leave the network on its own decision. Nodes in MANET should be able to discover their neighboring nodes to configure the dynamically changing network. At present, providing secure data transmission in MANETs is challenging task. MANETs are more vulnerable to security threats due to lack of centralized administration and they use free space to perform

communication with one another. So security is the essential component for any network. In fact, MANETs are more vulnerable to DOS attacks compared to wired networks because of its following characteristics

i) Dynamic Network Topology

MANETs have dynamically changing network topology because of node mobility. As the mobile node changes their position in the network that leads to continues change in the topology and route. There is a frequent partition of network takes place which may result in data loss [2].

ii) Limited Bandwidth

The bandwidth of MANET is limited in wireless networks as compared to wireless links.

iii) Limited Energy Resources

All the mobile nodes in MANET are equipped with battery, hence these devices have little capacity.

iv) Open medium

Generally, MANET nodes have freedom to join or leave the network without any constraint. A node in MANET can communicate with other node if it is in its range. Due to this it is more susceptible to attack [2].

v) Cooperative Algorithm

The routing algorithm of MANET is cooperative that requires the mutual trust between nodes [2].

vi) Lack of centralized administration

There is no any fixed infrastructure, hence this category of networks are prone to threats.

1.1 Denial of Service (DOS) Attacks

Dos attack is one that attempt to prevent the victim from being able to use all or part of the network connection [3]. DOS attacks have numerous forms all they are hard to prevent. For instance an attacker may send excessive amount of requests to a server that has test their legitimacy. This test requires an amount of CPU and memory capacity. Due to the excessive number of requests the server will be in testing illegal request and will be unavailable to legal users [3].

1.1.1Black Hole Attack

Black Hole attack is a type of DOS attack where a malicious node attacks all its neighboring nodes by falsely claiming a fresh route to the destination and drops them without forwarding them to the destination.

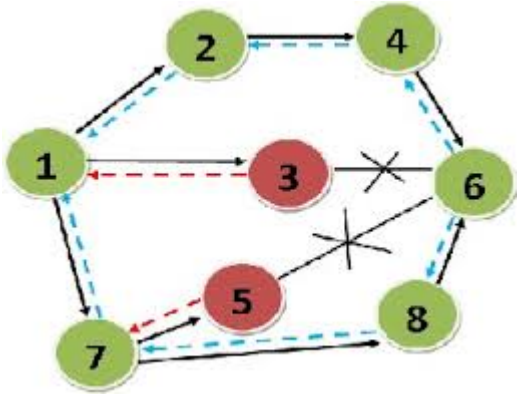


Figure: Black Hole Attack

The above figure shows how the black attack problem occurs. In the above figure, node A wants to send data packets to node D. in this, first path should be established between A and D. for this, node A broadcasts QRY packet to its neighboring nodes B and C. after receiving QRY message from node A, node C immediately respond and send UPD packet to node A, will

ignore another route reply from node B without checking the validity of path received from node C. then node C will drop the packets.

2. Review of Literature

There are many solutions developed for detection and prevention of Black Hole attack in MANET. Most of these solutions based on the methods reputation based, promiscuous monitoring, neighbor node detection and trust mechanism. Some excellent work has been done detection based approaches based on trust in MANETs [9]. The following are the different black hole attack detection and prevention techniques.

Marti et al. [6] proposed the use of Watchdog and path rater. Watchdog promiscuously listens to the transmission of the next node in the path to detect misbehaviors. Path rater keeps the ratings for other nodes ranges vary from 0 to 0.8 where 0.5 signifies node as neutral. These values are updated periodically by 0.01 each 200ms and performs route selection by choosing routes that do not contain selfish nodes. However, the watchdog mechanism needs to maintain the state information on the monitored nodes and the transmitted packets, which undoubtedly increases memory overhead.

Fidel Tachil et al [2] proposed a trust based approach for AODV protocol. in this approach every node monitors neighboring nodes and calculates its trust value. If this value goes below threshold value then the monitoring node considered as malicious node. The trust value of a node is calculated as a ratio of number of packets dropped to the number of packet forwarded by that node. The cache mechanism implemented by every node in order to confirm that data sent by it are being forwarded or not.

Pramod Kumar Singh and Govind Sharma [8] proposed method uses promicious mode to detect malicious node and propogates the information of malicious node to all the other nodes in the network. It does not require any database, extra memory and more processing power.

Nabarunchatterjee et al [2] proposed a triangular encryption technique for the detection of black hole attack. According to this approach source node send a plain text along with RREQ, when intermediate node receives a RREQ, it sends this packet to the destination node instead of RREP to the source node. Destination node encrypts the plain text with pre agreed partition with key and sends it with RREP. On receiving these packets intermediate node update their index and hop count. If the RREP packet contains cipher text it is sure to have reached the destination.

3. Proposed Trust TORA

In our proposed method, we implemented reputation based trust route mechanism to protect the MANET from black hole attack. For this we modified the TORA protocol to be able to detect and prevent multiple black hole attacks.

3.1 Reputation Based Trust Route Mechanism

In recent years, several trust reputation models have been proposed to handle the security of mobile ad hoc networks but they fail to capture evidence of trustworthiness within the limitations of the network [4].In this work, we adopted a reputation based trust route mechanism in TORA protocol to protect it from Black Hole attack. In our proposed method, the evidence is captured from interactions with neighbors, observing interactions of neighbors and through recommendations. The captured

evidence is then quantified and represented as reputation ratings. Evidence from interactions of neighbors is captured in order to identify the nodes that are likely to misbehavior during an interaction. Finally, the quantified evidence is represented as direct, observed and recommended reputation ratings. Reputation-capture and reputation-evaluation modules are developed to perform the operations [4].

4. Trust-Evaluation

Trust-evaluation performed at a node depends on the following factors-the position of the evaluating node, type of event and the context in which the evaluation is invoked. Note that the evaluating node may be source or destination or an intermediate node. Event types include route request, route reply, route error and data flow event. The context is a combination of decision policies.

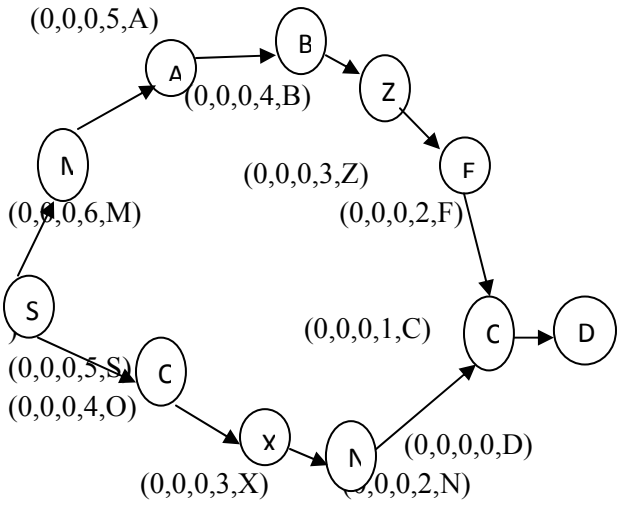


Figure 1: Route Creation in TORA

Let us consider the above scenario, in which intermediate node N has to decide whether to forward or ignore a received packet. Initially, the trust evaluation module extracts the nodes from the route, the position of extracted nodes are follows source, destination, prev-hop and next-hop. Now the trust-valuation module calls the trust-over-reputation module to compute the trust for nodes.

The trust-evaluation module then computes trust for packet by combining the trust values received for nodes S, D, X, and C from the trust-over-reputation module.

$$T_N\ Packet_{(}t_a+1) = \sum I_{N\text{-}list} * T_N\ Node_{list}(t_a)$$
$$\sum I_{N\text{-}list}=1$$

equation (1)

Where

List={source, destination, prev-hop and next-hop}

The trust computation $T_N\ Packet_k(t_a+1)$ for a packet k, by node N at time t_a+1

$I_{N\text{-}list}$ defines the importance given to the trust of an extracted node depending on the nodes' position in the route. Finally, the trust-evaluation module forwards the packet only if the trust for the packet is at least the threshold-limit (Δ) [4].

4.1 Trust-over-reputation

As mentioned in the trust-evaluation, the trust-over-reputation module computes trust for a node. Recall that trust is derived from the reputation ratings which represent the quantified evidence.

Hence, all the three types of reputations (direct, observed and recommended reputations) held for a node is combined into an overall-reputation to represent the trust for that node.

$$T_N\ Node_i\ (t_a+1) = \sum U_{N\text{-}i}^{type} * \square_{N\text{-}I}\ type(t_a)$$
$$\sum U_{N\text{-}i}^{type}=1$$

Equation (2).

Where,

$T_N Node_i(t_a+1)$ represents N's trust for I at time t_a+1

$\square_{N-I}$ type(t_a) refers to the N's reputation of type 'r' for 'I' at time t_a

U_{N-i}^{type} signifies the utility of each reputation type during the trust computation for a node.

Type={direct, observed or recommended reputation}.

Now we detail the steps involved in capturing, quantifications and representing the evidence as reputation ratings by using the capture-reputation and reputation-evaluation modules [4].

4.2 Direct Reputation

Direct reputation for a node is based on the evidence that is captured and quantified form one-to-one interactions with the node. To capture evidence, the reputation-capture module verifies the overheard packet against copy the packet stored in the packet-buffer. A positive or negative value is assigned to the capture evidence, and referred as the new direct reputation. The new direct reputation then passed to the reputation evaluation module along with the identity of the node for which the stored direct reputation in the reputation-table has to be revised [4].

A positive value pos (event), is assigned for the captured evidence, only if the packet has not undergone any malicious action. The magnitude of the value depends on the type of event. Alternatively, a negative value, Neg (event, action) is assigned, if the captured evidence confirms a malicious action. In case of malicious action, the malicious next-hop is added to the reject list in order to exclude from the communication path. The reputation-evaluation module dumps the new direct reputation in to the stored direct reputation to arrive at the revised direct reputation. The revised direct reputation then becomes the stored direct reputation for future operations [5] the operation is summarized in the following equation.

$$\square_{N-i}^{Direct(t_{a+1})} = \begin{cases} \min\{1, |\square_{N-i}^{Direct(t_a)} + pos(event)|\} & \text{if 'i' is benign;} \\ \max\{-1, |\square_{N-i}^{Direct(t_a)} - neg(event, action)|\} & \text{if 'i' is malicious;} \end{cases}$$

Equation (3)

Where,

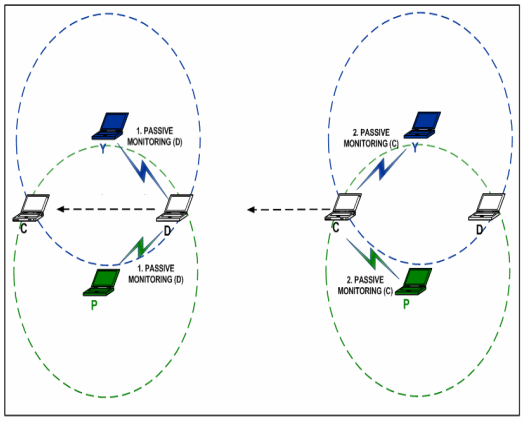
$\square_{N-i}^{Direct}(t_a)$ is the stored direct reputation held for 'i' by N at time 't_a'

4.3 Observed Reputation

Observed reputation is defined as the opinion held by a node towards an observed node depending on the captured and quantified from the observed node's behavior towards a common neighbor.

Consider the scenario as shown in the following figure, where nodes P and Y update the observed reputation of C based on the interactions observed their neighbors D and C. to begin with P and Y overhear the packet forwarded by D to C, and then the packet forwarded by C on behalf of D. nodes P and Y discard the observed evidence if C has forwarded the packet without modification. From the perspective of P and Y, C forwarding D's packet is not only an instance of normal behavior, but also relatively insignificant. Furthermore, the decision to discard the

evidence there was observed for normal behavior assists in counteracting colluding attacks. Otherwise, D and C may exchange dummy packets between to increase their observed reputation at P and Y. an exception to this rule applies if C generates a route error whenever D becomes unreachable. Note that the creation of a route error can be considered as extraordinary behavior in a resource-constrained MANET. On the other hand, P and Y assign a negative value for C, if C has performed a modification attack. The negative value is proportional to both the type of event and the attack. Node C is appended to their reject-list for exclusion until the completion of the corresponding communication flow. Node C not only loses direct reputation at its previous hop D for each of its misbehaviors, but also the observed reputation at all the observing neighbors including Y and P.



The following is the equation for calculating observed reputation

$$\square_{N-i}^{Observed(t_{a+1})} = \max\{-1, |\square_{N-i}^{Observed(t_a)} - neg(event,action)|\}$$

if 'i' is malicious;

Equation (4)

Note that a node not only loses its direct reputation at the previous-hop for misbehavior, but also the observed reputation at all observing neighbors.

Recommended Reputation

Recommended reputation is defined as the indirect opinion held by a mobile node to- wards another mobile node based on the derived recommendations. A mobile node that provides recommendations is referred to as a recommender. Likewise, a recommended node is referred as a recommendee, and a mobile node that receives recommendations is known as the requesting node.

Both the direct and observed reputation capture can only enlist malicious nodes into the reject-list apart from capturing the evidence, but cannot prevent the propagation of maliciously modified packets during route discovery.

Let us consider the scenario as shown in the figure 1, containing the route S->O->X->N->C->D. as mentioned earlier, N forwards the received packet, only if the packet passes all the trust evaluations. Subsequently to successful evaluations, the reputation-capture at N derives X's willingness to forward the packet on the behalf of O, as X is recommending O. similarly, it derives O's willingness to forward the packet on behalf of S as O in recommending S. the process of deriving recommendations from the route terminates at S as there is no previous-hop for S. Let us consider the recommendation derived from X for O at N. first, the trust for X

is computed using equation (2). Depending on whether N's trust for X is at least the threshold-limit (delta), the reputation-capture module assigns a pre-determined positive or negative value for the derived recommendation. This only demonstrates N;s view on the recommendation derived from X for O. however, it does not differentiate the positive or negative recommendations derived for other nodes. The differentiation is necessary because N's trust for X need not be the same as its trust for representing the recommendation derived from X for O is scaled by N's trust for X to arrive at the new recommended reputation for O. finally, the reputation-evaluation module computes the revised recommended reputation for O by integrating the recommended reputation into the stored recommended reputation held for O. the same procedure is then repeated recursively for the recommendations derived from O to S.

$$\square_{N\text{-}O}^{Rec(t_{a+1})} = \begin{cases} \min\{1, |\square_{N\text{-}O}^{Rec(t_a)} + T_N Node_x(t_a) * pos(action)|\} & \text{if } T_N Node_x(t_a) \geq \Delta \\ \min\{1, |\square_{N\text{-}O}^{Rec(t_a)} - T_N Node_x(t_a) * neg(action)|\} & \text{if } T_N Node_x(t_a) < \Delta \end{cases}$$

Equation(5).

5. Simulation Results

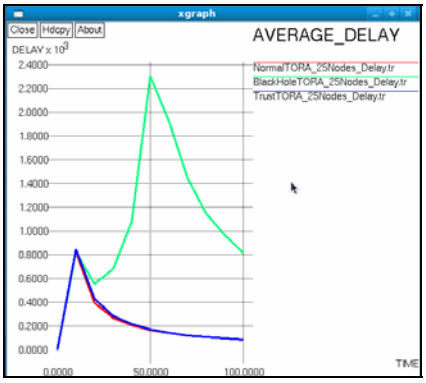


Figure: Average Delay Comparison for Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 25 Nodes

As shown in the above graph, Average Delay of Normal TORA and Trust TORA are similar but TORA under black hole attack take more delay.

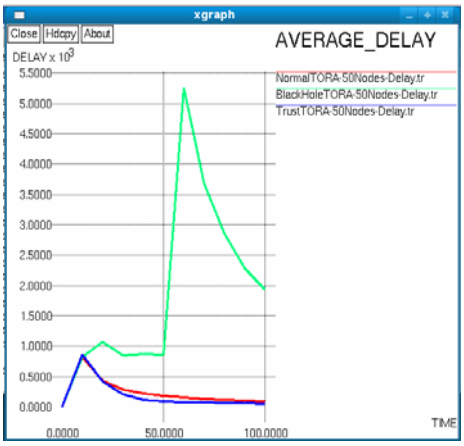


Figure: Average Delay Comparison for Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 50 Nodes

As shown in the above graph, Average Delay of Normal TORA and Trust TORA are similar but TORA under black hole attack take more delay.

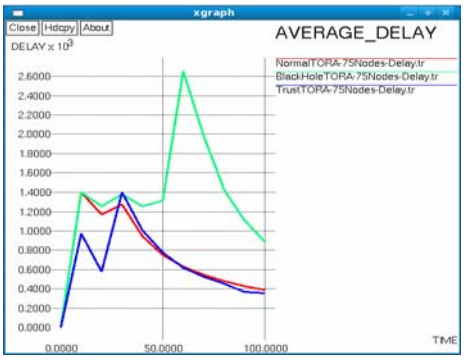


Figure: Average Delay Comparison for Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 75 Nodes

As shown in the above graph, Average Delay of Normal TORA and Trust TORA are similar but Normal TORA take slightly more delay up to simulation time 50 sec. TORA under black hole attack take more delay.

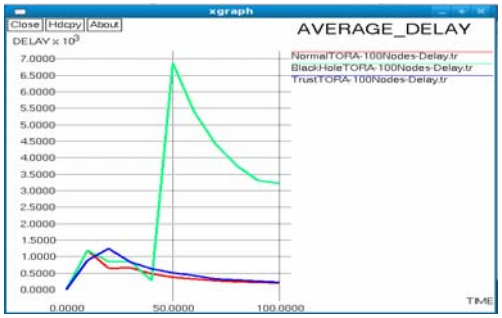


Figure: Average Delay Comparison for Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 100 Nodes

As shown in the above graph, Average Delay of Normal TORA and Trust TORA are similar but Trust TORA take a little bit delay at some intervals of simulation time .TORA under black hole attack take more delay.

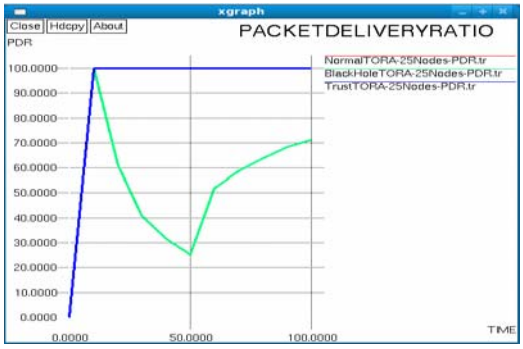


Figure:Packet Delivery Ratio Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 25 Nodes

As shown in the above figure, Noraml TORA and Trust TORA possess the same Packet delivery Ratio. TORA under black hole attack posses low packet delivery ratio while the attack is active.

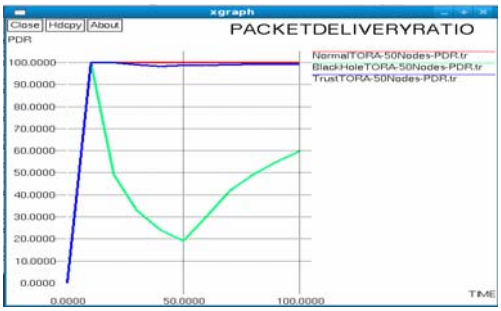


Figure:Packet Delivery Ratio Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 50 Nodes

As shown in the above figure, Noraml TORA and Trust TORA possess the same Packet delivery Ratio. TORA under black hole attack posses low packet delivery ratio while the attack is active.

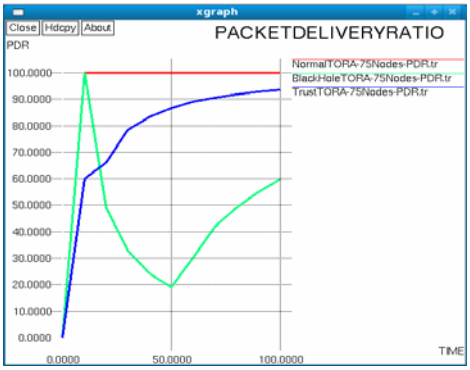


Figure:Packet Delivery Ratio Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 75 Nodes

As shown in the above figure, Noraml TORA and Trust TORA possess the same Packet delivery Ratio. TORA under black hole attack posses low packet delivery ratio while the attack is active.

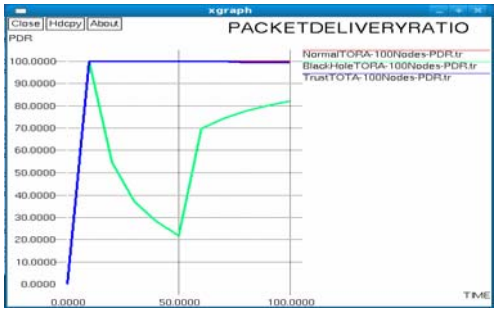


Figure:Packet Delivery Ratio Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 100 Nodes

As shown in the above figure, Noraml TORA and Trust TORA possess the same Packet delivery Ratio. TORA under black hole attack posses low packet delivery ratio while the attack is active.

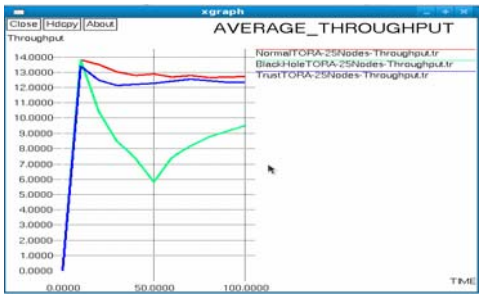


Figure:Throughput Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 25 Nodes

In the above graph, throughput of all the three protocols starts steadily, but throughput of TORA under black hole attack gradually decreases. Throughput for Normal TORA and Trust TORA are almost similar.

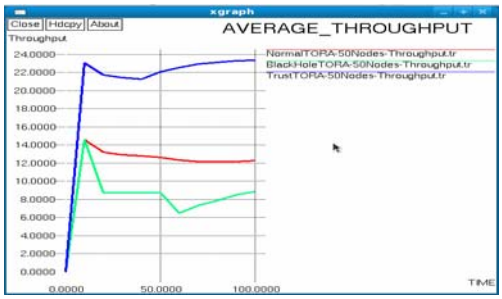


Figure:Throughput Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 25 Nodes

In the above graph, throughput of all the three protocols starts steadily, but throughput of TORA under black hole attack gradually decreases. Throughput for Normal TORA and Trust TORA are almost similar.

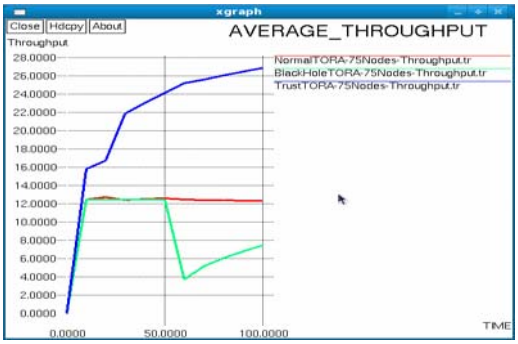


Figure:Throughput Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 25 Nodes

In the above graph, throughput of all the three protocols starts steadily, but throughput of TORA under black hole attack gradually decreases. Throughput for Normal TORA and Trust TORA are almost similar.

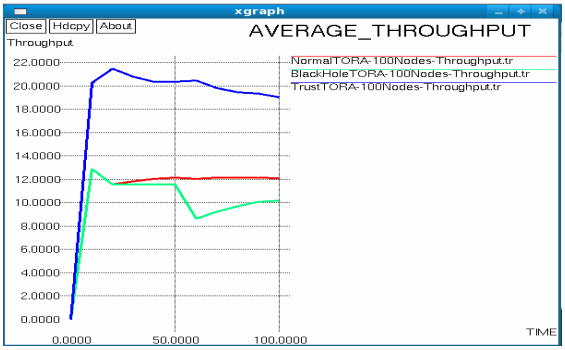


Figure:Throughput Comparison of Normal TORA, TORA under Black Hole Attack and TrustTORA for Network size 25 Nodes

In the above graph, throughput of all the three protocols starts steadily, but throughput of TORA under black hole attack gradually decreases. Throughput for Normal TORA and Trust TORA are similar.

6. Conclusion

We implemented reputation based trust route mechanism to enhance the security of wireless network under harsh conditions. To carry out our research we selected on-demand routing protocol TORA. Our proposed Trust TORA performs well in terms of Delay, PDR and Throughput than TORA under black hole attack.

In this work, we implemented only black hole attack, the future work may be simulation of various DOS attacks using TORA.

7. References

[1] S.B Aneith Kumar, S. Allain Devaraj & J. Arun Kumar,"Efficient Detection of Denial of Service Attacks in MANET",IJARCSSE,2012, PP 470-475.

[2] Rahul Kumar and Monika Sachdeva," A REVIEW OF DIFFERENT BLACK HOLE DETECTION TECHNIQUES IN MANET", vol 1, Spl Issue 2, ICRTEDC-2014.

[3] Safdar Ali Soomro, Sajid Ahmed Soomro, Abdul Ghafoor Memon and Abdul Baqi," Denial of Service Attacks in Wireless Ad hoc Networks", Journal of Information & Communication Technology, Vol. 4, No.2, 2010.

[4] Venkat Balakrishnan, Vijay Vardhan, Phillip Lucs and Kiran Tupakula, " Trust Enhanced Secure Mobile Ad hoc Network Routing", Advanced Information Networking and Applications Workshops,2007,AINAW,21st Information Conference on Vol.2.

[5] U.Venkanna and R.Leela Velusamy,"Black Hole Attack and Their counter measure based on Trust management in MANET: A survey", Proceedings of International Conference on Advances in recent Technologies in Communication and Computing, 2011.

[6] Poonam Gera, KumKum Garg, and Manoj Misra, " Trust-Based Multipath Routing for Enhancing Data Security in MANETs", International Journal of Network Security, Vol. 16, No.2,PP.102-111, Mar. 2014.

[7] Sarita Badiwal and Vandna Verma,"Survey of IDS in MANET against Black Hole Attack", International Journal of Application or Innovation in engineering & Management (IJAMEN), Vol.2, Issue 5, May. 2013.

[8] Shashi Gurung, Aditya Kumar and Kumar Saluja," Survey of Black Hole Attack Detection in Mobile Ad Hoc Networks", Proceedinds of International Joint.Conference, 7th july 2013,Goa,India.

[9] 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", DOI 10.1109 TVT.2014.2313865, IEEE Transaction Vehicular Technology.

[10] Eman Farag Ahmed, Reham Abdellatif Abouhogail and Ahmed Yahya," Performance Evolution of Black Hole attack on VANETs Routing Protocols", International Journal of Software Engineering and its Applications Vol.8, No.9, 2014.