# Transmission of Secure data using Cryptograph Technique in MANETs

[1]Anuradha T, [2]Saroja

[1]Dept of CSE, PDA College of Engineering Kalaburgi, India
[2]Dept of CSE, PDA College of Engineering Kalaburgi, India

*Abstract:* MANET is dynamic in nature without any fixed infrastructure and vulnerable to many kinds of attacks. The increased usage of wireless network and limited resource constraints of devices restricts the use of cryptography mechanisms for security in network. Safe data transmission along with data integrity and confidentiality are important aspects. To achieve these aspects the cryptography is a concept used to protect data from malicious nodes over untrusted network. The mechanisms based on trust are able to provide security in the network like access control. A scalable security overlay is designed over trust-based routing for detecting and providing security services from misbehaving nodes. This paper is about transmission of secure data from malicious nodes and increases the network performance by using concept of cryptography over untrusted network for secure data and results are analysed using ns2 simulator.

***Index Terms*** **- MANETs, Security attacks, Misbehavior detection, Trust and Cryptography techniques, Two fish, RSA.**

## I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a network of mobile nodes without fixed infrastructure connected using wireless links. Nodes are freely moving continuously change their position in this network any new nodes can join the network or leave the network, nodes may temporarily fail to connect wirelessly when the nodes are out off coverage range. In MANETS the mobile nodes have some limitations like limited capacities and short battery life and security issues. Security is the major issue in this kind of network and MANET is susceptible to several kinds of attacks such as DOS, rushing attacks, syn flooding etc. AODV is a standard protocol, where source node makes comparison of destination sequence number when it receives multiple route replays and decides greatest sequence number as route replay. If sequence numbers are same then it selects based on smallest hop count. This results that data transmission will move towards the malicious node and transmission will be dropped. Some security attacks are syn flood, black hole, sink hole, jellyfish attack, wormhole attack etc. DOS is problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its destination.

**Wormhole attack:**

In This type of attack malicious nodes have a tunnel between them. The attacker node captures data packets from one location and forwards to unauthorized node in other location. It is a kind of passive attack where attacker node causes unauthorized access and performs DOS attacks. If there is fast data transmission route between the ends of wormhole that tunnels the data transmission at high speed compared to the normal mode wireless communication. Thus wormhole attracts much more traffic in network from their neighbor nodes and results rushing attacks. In this rushing attack due to fast data transmission path all data packet follow the same path and this will lead to increasing attack success rate. Wormhole attack is dangerous and harmful to network**.** The figure 1 shows that the example of wormhole tunnel between nodes here source node S wants to send data to destination D. the wormhole node F attracts traffic in network from neighbor due its fast transmission nature. The node F has a connected node G. Node F sends the data pakets to unauthorized node G for malicious intension instead of forwarding to node D.

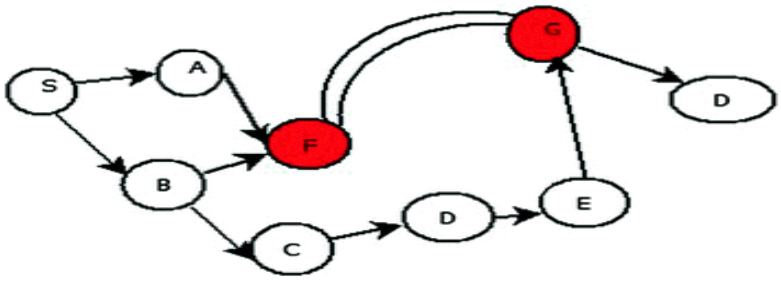


Fig. 1: Wormhole attack in MANET

**Blackhole attack:**

The blackhole attack is well known security attack in MANET. In this type of attack a malicious nodes advertises themselves as having shortest path to the node for those node they wants to intercept. A blackhole node replies that it has fresh and shortest route to the destination to the route request and then it drops the received data packets. Malicious nodes may work together in group and cause serious damage in network. The fig. 2 shows the example of black hole attack in mobile ad-hoc network here node x advertises that it has shortest path to destination to source node. The source nodes forwards data packet to black hole node. The node x drops the packet instead of forwarding

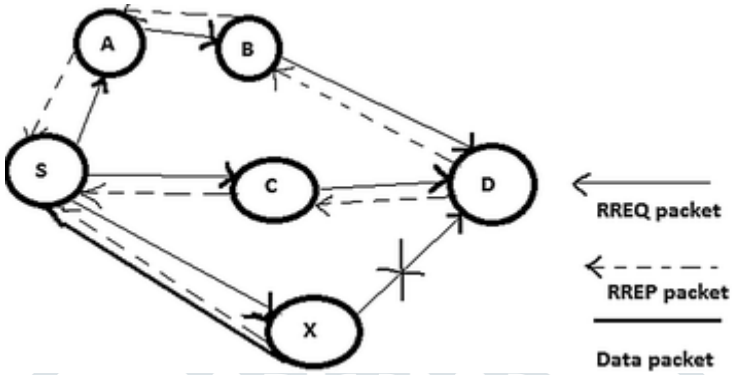


Fig. 2: Blackhole attack in MANET

## II. LITERATURE REVIEW

MANET is vulnerable to number of attacks such black hole attack Using AODV routing protocol these kinds of attacks can be reduced [1] this paper introduces new concept of self-Protocol Trustiness in detecting malicious behavior and they have presented new mechanism to resist black hole in the network here overhead in the network is reduced by avoiding cryptography or authentication mechanism. The concept of SAODV reduces the effect of black hole in the network and in [5, 9] here each node maintains their routing table for checking information about the neighbor node in order to find destination path, experiments are performed on ns-3simulator, AODV gives a route with loop-free and repairing if any broken links and this protocol maintains all advantages of routing mechanisms like basic distance vector and verified operations of algorithm. And in attack [2] a cryptographic technique is used for secure data transmission to reduce the effect black hole attack in this paper author recommended peer-to-peer symmetric encryption to reduce the packet loss in the network. Wormhole attacks in the MANET cause serious damage to network and nodes. These kinds of attack detection and prevention is discussed in [3] the aim of this work is to overcome a special kinds of attacks called wormhole. Detection and removal of wormhole attack is done by modifying the AODV protocol. WADP algorithm has been implemented on modified AODV. Where node authentication is able to detect the exposed wormhole attack along with WADP and modified AODV are able to remove hidden wormhole attack in the network. The security attacks with node mobility allow the network susceptible to Byzantine faults with packet misrouting, packet corruption or packet dropping Packet dropping. The solution is discussed in [4] the proposed solution using unobtrusive monitoring technique with "Detection Manager" to identify the malicious node which cause corruption and packet dropping. Cryptographic solutions have been used for security in network [7] for misbehavior detection used elliptic curve cryptography. EAACK with elliptic curve algorithm used for intrusion detection system to maintain data integrity, authentication and for non repudiation protocol used IDS. Safe data transmission using cryptographic technique [10] a visual cryptography method has been proposed they have used the concept of steganography for information hiding and used tiny encryption calculation for information encoding in this method the information will experience security using tiny encryption then hiding data behind the images for secure information from the attacker. DES encryption with length of key is 56 bits consists two attributes: substitution method and transportation [8]. DES with small size of key is considered insecure in many areas [6] DES is vulnerable to some attacks such as Linear Cryptanalysis. RSA is an asymmetric encryption standard because of large and asymmetric key this technique is secure for decades of years. Delay tolerant networks captured attention due to the growing importance and usage of these networks in challenging environment. For exploiting contact opportunity most of the designed routing protocols for oppNets use the nodes mobility. The routing based on utility metrics has been discussed in [5] provides the CAN-based routing which are utility driven which are able to forward the message to nodes with higher utility. The routing based on CAN uses the utility metrics such as, similarity, betweenness, contact frequency, and last encounter time. Social selfishness problems in delay tolerant networks discussed [11] in delay-tolerant network most people wants to forward packets to specified nodes but not all or other nodes. So for this kind of social selfishness proposed a routing algorithm which is Social Selfishness Aware Routing (SSAR). This improves the performance and allows the selfishness. The human involvement in oppNets is able to use trust of network nodes for cooperation enforcement, and selfishness discouragement. The participation and cooperation of network nodes leads to success of Oppnets. In [12] the trust based incentive schemes are designed for discouraging selfishness and enforcing cooperation in the network. In [13] this paper they have proposed a computation stargy i.e., Adaptive Trust Threshold (ATT).According to the condition of network such as node degree, node connectivity, trustworthiness of neighbor node and link changes. Identification of topology factors affect the trust threshold at all node, build a mathematical model for Adaptive trust computation. ATT achieves significant improvements in PDR and increases the detection

rate. The proposed adaptive threshold stargy can be implemented over the any trust based scheme which allows nodes to optimize the trust threshold. Protocol used is OLSR and evaluation made with NS2 under different network conditions. This proposed stargy achieves high throughput, improved packet delivery ratio, increased detection rate compared to traditional trust thresholds approaches. Routing in DTN is challenging since it must handle partitioning of network, long delay, and dynamic topology in such networks. In recent years social based approaches attempts to improve performance of routing is discussed in[14] these methods take the advantages of positive social charters tics. In this article, they have discussed different social characteristics of nodes to improve the routing in DTN. Made comparison of routing protocols such as SimBet, Bubble Rap, Social Based multicasting, SSAR etc. from the analysis and comparison of these methods conclude that social based approaches are more prominent than opportunity based routing protocol for DTN. The trust-based routing protocol for secure communication in MANET & WSN is discussed in [15] Trust and security are achieved by the node's trust factor maintenance. This factor is established over time and it increases for each node when it participates successfully in data transmission. Trust of discovered multi hope paths between source and destination is important to achieve the security communication. The simulation results showed improvements in trust of discovered path with the choice of important trust parameters. Two versions of routing protocol, TRAS-25 & TRAS-50 are compared with each other and DSR routing protocol.TRAS-50 performed best than TRAS-20 and DSR. This protocol operates on a reward model and does not directly penalized nodes that do not participate in the data transmission or are malicious in process.

## III. PROPOSED SYSTEM

In this paper, a cryptographic technique is proposed along with trust-based security model in the MANET for secure data transmission. The trust-based routing with cryptographic means in network supposed to cater the identification and isolation of malicious nodes in the network. The security framework in this work is designed to detect the wormhole attack and black hole attack in the network. The established symmetric and asymmetric key cryptography provides authentication, confidentiality and integrity in the network. RSA and Twofish algorithms are used for encryption purpose. Comparisons are made between these two algorithms and conclude that Twofish is effective and efficient then the RSA, results and discussion shown in NS2.

### 3.1 Design

For providing hop-to-hop authentication, Two-fish algorithm, RSA algorithm and concept ECDSA considered. The design provides a solution based on infrastructure, to maintain the message integrity, hop-to-hop authentication and detection of malicious node in the network. This work targeting black hole attack and wormhole attack. By considering the security framework, the nodes in the network are classified as normal behavior node (i.e., nodes having no malevolent intent), malevolent nodes (i.e., the nodes having malevolent intent), intelligent spy nodes (i.e., the nodes are capable for collecting evidence against malevolent) and judge nodes (i.e., the nodes having ability to judge the malevolent node behavior).

Intelligent spy nodes and judge nodes are infrastructure nodes. They are assumed as uncompromising nodes. The trust based routine protocol with the trust adjustment factor used in trust calculation of node.

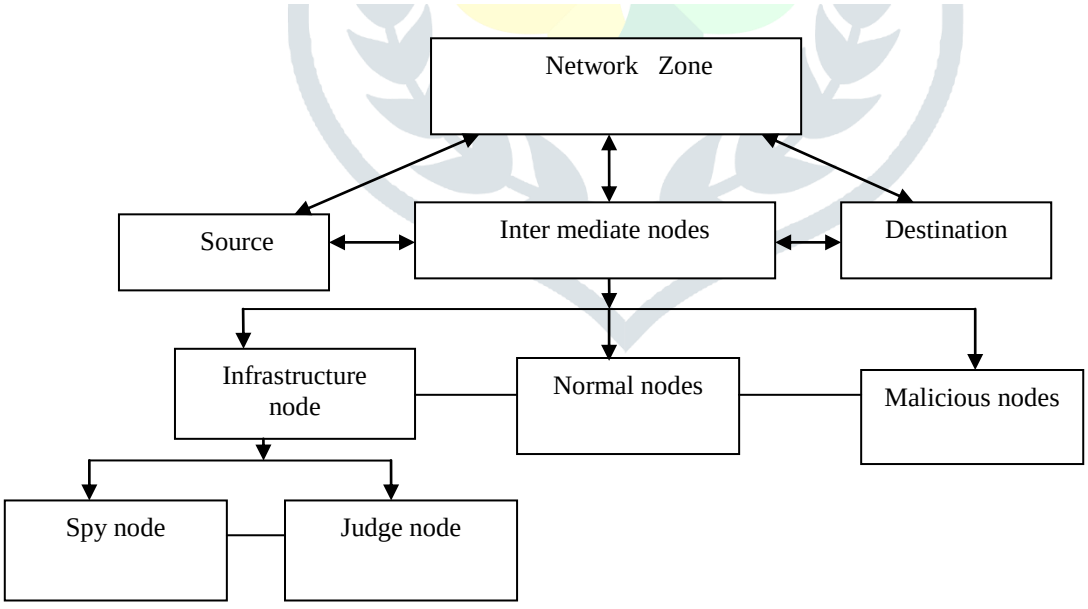


Fig. 3: Proposed System Architecture

The fig.4 shows the data flow of our proposed approach

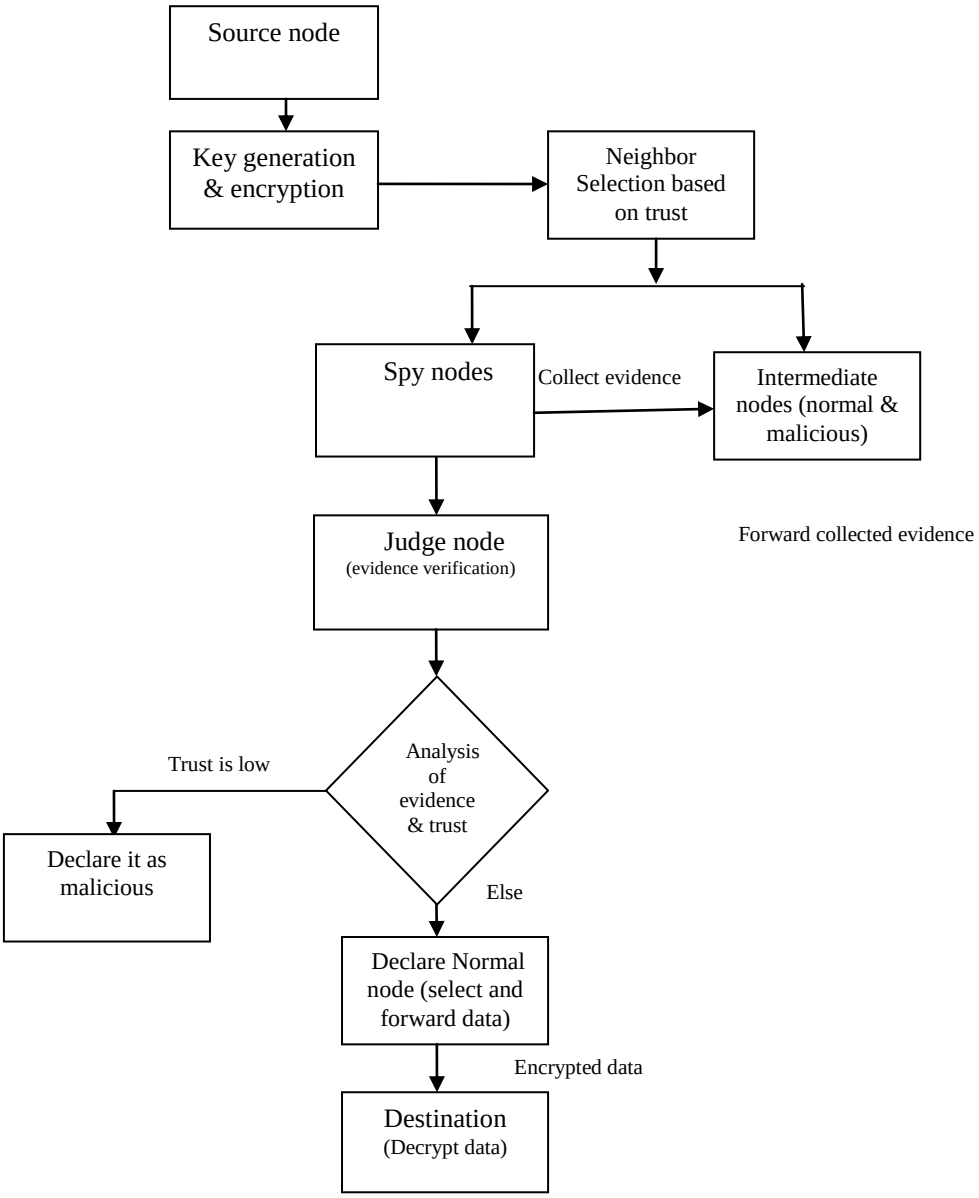


Fig. 4: Flow diagram of proposed approach

**3.2 Security Model**

A Security scheme is designed for protecting the normal nodes from malevolent nodes. The intelligent spy nodes and judge nodes play the important role in protecting and providing security in the network. The intelligent spy nodes collect the evidence of malevolent nodes and send it to the judge nodes. Based on the evidence, judge nodes give the judgment. The designed security overlay is infrastructure based and it has been classified into two components:

a. Node component with physical intelligence : The responsibility of intelligence nodes in the network is to provide security. The action of these intelligent nodes in the network is to collect the evidence and evaluate the evidence against the malevolent entity. The network area is divided into number of zones and each zone is assigned with spy team compromising the number of spy nodes. This spy team is monitored by a single judge node. The number of spy nodes depends on mobility of normal nodes in the zone.
Let us consider the area of network having length “l” and breadth “b”. The total area of network l*b is divided into N number of zones. The division of network is two types length wise and breadth wise is N1=BP/X & N2=L/XB respectively. X is user constant.

The area is divided into N = ((N1+1)*(N2+1)) zone.

b. Logical cryptographic based component: To provide message integrity, confidentiality and authentication in the network, the cryptographic algorithm is used. It ensures the application of cryptographic algorithm at hop-to-hop level, also ensures the authentication. The hop-to-hop authentication in the network is ensured through Twofish algorithm.

Classification of nodes in the network

- **Normal behaviour nodes**: The normal nodes are easily prone to attacks. So, it is essential to provide security to these nodes. These nodes use trust based routine protocol over which security framework is implemented.

- **Spy nodes**: In network, each zone is associated with a spy team compromising spy members and spy heads. Spy nodes responsibility is to collect the evidence against malevolent nodes and then defending these accusations in front of judiciary. The target of spy team is complete zone, a set of nodes or any single node. The digitally signed in and out timestamp of message is appended by each normal node in message payload. These digitally signed timestamps are verified by the immediate neighbors in the network. The message payloads are used in a way to get the information about malevolent behavior of node in the network. The malevolent behaviour is targeted on two levels – node level and message level. The malevolent behavior at node level is addressed through team surveillance of spy nodes. The spy members share the collected spy information with team heads. Through message follow-up operation, surveillance is carried out in the other way. The collected information is calculated for loop formation over delay, wormhole pattern, black hole pattern and time to live lost. The collection of evidence is done through locating and positioning these nodes for fallow-up operations, node fallow-up and message fallow-up. The spy nodes works under self induced and judge induced surveillance mode. In each mode primary task is to collecting evidences against malicious nodes. The evidence are message forward list, message received list, duration of contact, speed, ttl, delay, coverage, data size and time stamp of every node and head spy node submits collected information to judge node of the zone for verification.
  The number of nodes in spy group is discussed here. The dimension of zone with length x and breadth y, the transmission range R.
  Each node covers a transmission area $\pi R^2$. By considering average number of spy nodes involved in zone be "n" the average of covered region is $n\pi R^2$.
  The average region not covered is zone's black shed area i, e
  $xy- n\pi R^2 = 0$
  $n = xy/ \pi R^2$. By assuming p% of total zone is black shed then

  $$pxy/100 = xy-n\pi R^2. \quad (1)$$

  So $n = xy(100-p)/100\ \pi R^2$.
  From this we can get the number of spy nodes. By the introduction of mobility in the network reduce the black shed area in the network.
  Consider u be reduction of black shed area in zone then (p-u)%of $xy = xy- n\pi R^2$.

  $$n = xy(100-p+u)/100\ \pi R^2. \quad (2)$$

- **Judge node**: The judge nodes are part of judiciary wing of infrastructure. These nodes coordinate the spy heads in their area of jurisdiction. The spy heads responsibility is to collecting information for evidence against malicious nodes and shared with judge node. The judge node considered as supreme authority for verifying the evidences collected by spy nodes in network. The judge node analyzes these evidences helps for judging and authenticates the collected evidences. These nodes verify evidences against malicious nodes. The perspective analysis of submitted evidences helps in figuring out the malicious intent of nodes in the network. The judge nodes verdict after properly establishing the evidence and facts for black hole, wormhole, TTL lost, and over delay. The judge nodes have authorization for routing and security data structure from any type of node in network. At node i the judge node checks MSG_ENC_LIST and then looks for the paired message ids for which the destination of one message id is the source for other message id and vice-versa. The mobility of judge nodes in jurisdiction zones helps in thwarting the attack and disseminating the malicious information in the network.
- **Twofish algorithm(Encryption)**
  A large amount of malicious behaviour can attack the network transmission at any time the Twofish algorithm provides key dependent S-boxes rules with 128 bit keys. These confirm that all S-boxes are strong enough. Twofish algorithms don't involve weak key support.
  The sub keys are calculated carefully using the rules of S-box to avoid the various key attacks and to provide good key integration. The byte arrangement takes place during 1-bit turning round, this process exists for to disturb the activity of cryptanalysts. Because 8-XOR is less than a round, it makes to leave them. There are several tradeoffs presents between key establishment and encryption time. Twofish provides key generation with key dependent S-boxes and sub keys as its high speed. Using Twofish algorithm it is possible to encrypt large volume of data with fast altering keys.

### 3.3 Communication between nodes

The main strength of this designed framework is communication among the infrastructure nodes. The desired attributes for infrastructure are speed, reliability, integrity, robustness and authority.The cryptographic component ensures the integrity, reliability, and authentication framework. The mobility pattern of infrastructure node ensures the speed and robustness in the design of security. The communication of infrastructure nodes is divided into intra node communication and inters node communication. Exchange of information among same type of infrastructure node in the network is intra node communication. And exchange of information among different types of infrastructure node is inter node communication.

The normal nodes maintains node encounter vector $EV_i$ with respective time. The $EV_i$ consists node id, time stamp $Tim_i$, message encounter lists MSG_ENC_LIST, message forward list MSG_FOR_LIST and request vector $R_{i,}$ for spying against doubtful activity at time $t_{0,}$ the time for judgment is $t_{k.}$ the elapsed time $E_{time}= t_k-t_{0.}$ The spy nodes fallow up the nodes and keep up surveillance vector $SV_i^t$ at time t.

The intra node communication under normal routing operation, where normal behavior nodes are communicates with other normal nodes and disseminates information about malicious nodes. The judge node communicates with each other for ranking and grading information about spy teams. The spy node to spy node communication for exchange of information obtained during spying operation.

### 3.4 Trust

The proposed security overlay over trust based routing used in the network. The nodes in network find the trust about other nodes of the network based on the interaction and observation of the behavior of node during data forwarding. The trusted nodes are selected as intermediate nodes for routing and data forwarding between source and destinations. This routing provides the social security, the designed security framework provides cryptographic security as well. The designed security mechanism identifies and isolates the malicious nodes in the network along with it also affects the trust of malevolent nodes using the factor TAF. The judge nodes verify the evidences and give their verdict against the malicious nodes. The judge nodes specify the scale of trust. The scale of trust is responsible for ascertaining the TAF.

TAF α (Scale of Trust of node i).

The TAF is used for trust calculation of node. The integrity of message about TAF is ensured using cryptographic means.

Trust = Message forward count between neighbors/ message received between neighbors.

## IV. ALGORITHMS

### i. Communication algorithm

Step1: Normal nodes maintains node encounter vector *EVi, message encountered list MSG_ ENC_Listi* , message forward list *MSG_For_ Listi*

step2: Spy nodes analyze *EVi, MSG _EN _Listi* , *MSG_ For_ Listi* for any disbelieving or doubtful activity of encountered nodes.

step3: If any doubtful activities of node are found it maintain those doubtful nodes list as suspicious list *S Listi* [ ].

step4: For these suspicious list *S Listi* [ ] nodes maintain $R_i$ and communicate with the concerned Judge node regarding spying request through encrypted edevidences.

step5: The judge node extracts the evidence using its decryption key [*EVi , MSG ENC Listi , MSG For Listi* ]

step6: Judge node requests the zone's head spy node for Black list and Surveillance list using cryptography

step7: Zone's Spy head respond and send [*SVi* and *Black_List*].

step8: On receiving all the evidences (judge [*EVi ,MSG _ENC_ Listi , MSG_ For _Listi* ]) and judge[*SVi* and *Black_List*], Judge verifies the evidences.

step 9: On completion of the verification process, the judge node verdict either in terms of Genuine Request or Bogus Request

step10: If (*verdict==Bogus_Request*) then depreciate the trust of the requesting node by constant amount *z*.

step11: If (*Verdict==Genuine*) then the concerned judge deploys the spy team $ST_k^i$.

step12: On receiving the notification, the spy team *STik* adjusts its mobility as per the target message/node follow-up operation. Gathers, arranges and gains information about the target message/ node. Maintains the evidences and digitally signed evidences and on encounter with judge node shares [*Evidences*].

Step13: On receiving [*Evidences*], the judge node extracts the evidences and decides for reverification of evidences.

step14: If the judge node decides for reverification then repeat steps 11, 12, 13.

step15: If the judge node verdicts out in favor of an appellant normal node, first the trust of the appellant node is increased by a constant amount *z* and then the nature of maliciousness is figured out, i.e., *Blackhole, Wormhole.*

**ii. Twofish algorithm**

1) Accept any key lengths up to 256 bit.
2) Encrypt the data in less than 500 clock cycles per block on Intel Pentium, Pentium Pro and Pentium II, for a fully optimized version of the algorithm.
3) Able to form 128-bit key (for optimal encryption speed) in a time less than the time required to encrypt 32 blocks on Pentium, Pentium Pro and Pentium II.
4) Does not use operations that make Twofish inefficient on microprocessor except 32-bit, 8 bit microprocessor and 16 bit microprocessor.

The implementation of Twofish cryptographic algorithm is used in ordered to increase safety in MANET. Twofish uses a 16-round Feistel-like structure with extra whitening of the input and output. Plain text is divided into four 32-bit words in the input whitening step. These input words are then xored with four key words.
Steps involved in Twofish Algorithm are as follows:

Step1: 16 bytes of Plaintext (128-bits), $P_{0 \ldots} P_{15}$ are first split into 4 words P0,……, P3 (32-bits each)
$P = \sum_{i=0}^{3} P(4i + j)2^{8j}$ i=0,.., 3
Step2: Input whitening step: these 32-bit blocks of plaintext is
XORing with sub-keys $R_{0,I} = P_i$ xor $K_i$ i=0,…3
step3: First two words & the round number is given as input to the function F.
Step4: The third word XOR the first output of F and then rotated right by one bit.
Step5: The fourth word is rotated left by one bit and XOR second output word of F.
Step6: Finally the two halves are exchanged.
$(F_r,0,F_r,1) = F(R_r,0,R_r,1,r)$ r=0,….15
R is used to select the appropriate sub-key for the F function.
Step7: Finally, after swapping
$R_{r+1}, 0 = ROR (R_r, 2 XOR F_r, 0, 1)$
$R_{r+1}, 1 = ROL (R_r, 3, 1) XOR F_r,1$
$R_{r+1}, 2 = R_r, 0$
$R_{r+1,} 3 = R_{r,} 1$
Step8: Output whitening step: undoes the swap o last round and XORing with sub-keys
$Ci = R_{16}$, (i+2) mod 4 XOR Ki+4 i=0,…3.
C0,…,C3 of cipher text 128-bit cipher text Ci
$Ci = [C [i/4]/ 2^{8( i \bmod 4)}] \bmod 2^8$ i=0,…15

## V. SIMULATION ENIVIRONMENT

| | |
|---|---|
| Channel | Wireless channel |
| Propagation | Two Ray Ground |
| Network interface | Phy /wireless Phy |
| MAC | Mac/802_11 |
| Interface queue | Queue /Drop Tail / pri queue |
| Link layer | LL |
| Antenna | Antenna/Omi Antenna |
| Queue length | 50 |
| Number of nodes | 20 |
| Simulation area | 500*500 |
| Traffic | CBR |
| Packet size | 512 |
| Topology | Flat grid |
| Initial energy | 100 joule |

## VI. RESULTS AND DISCUSSIONS

This section deals with performance analysis of network. The simulation area is divided into number of zones. The infrastructure nodes deployed in each zone for detecting malicious nodes. The normal and malicious nodes are distributed throughout the network. Spy and judge nodes are able to detect the malicious node in the network. The established cryptographic mechanisms (Symmetric and Asymmetric) provide the authentication, confidentiality and integrity in the network. The comparisons made between misbehavior detection and secured data transmission using Twofish algorithm with cryptography based misbehavior detection using RSA algorithm.

CTSDTT-Cryptography Technique to Secure Data Transmission using Twofish.

CTSDTR- Cryptography Technique to Secure Data Transmission using RSA.

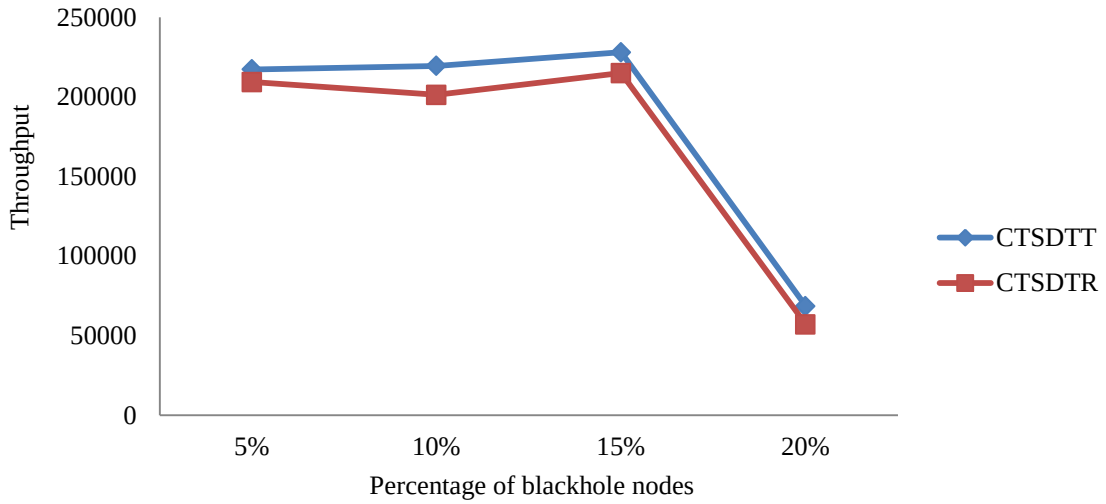


Fig. 5: Throughput comparison of CTSDTT & CTSDTR by Setting Number of Nodes in Different Percentage.

In data transmission, network throughput is the amount of data moved successfully from one place to another in a given time period the Fig. 5 shows the comparison of cryptography technique to secured data transmission using two fish algorithm (CTSDTT) and cryptography technique to secured data transmission using RSA (CTSDTR). The tests are made by setting the number of nodes in different percentage for both algorithms. The Two fish algorithm shows higher throughput than the RSA

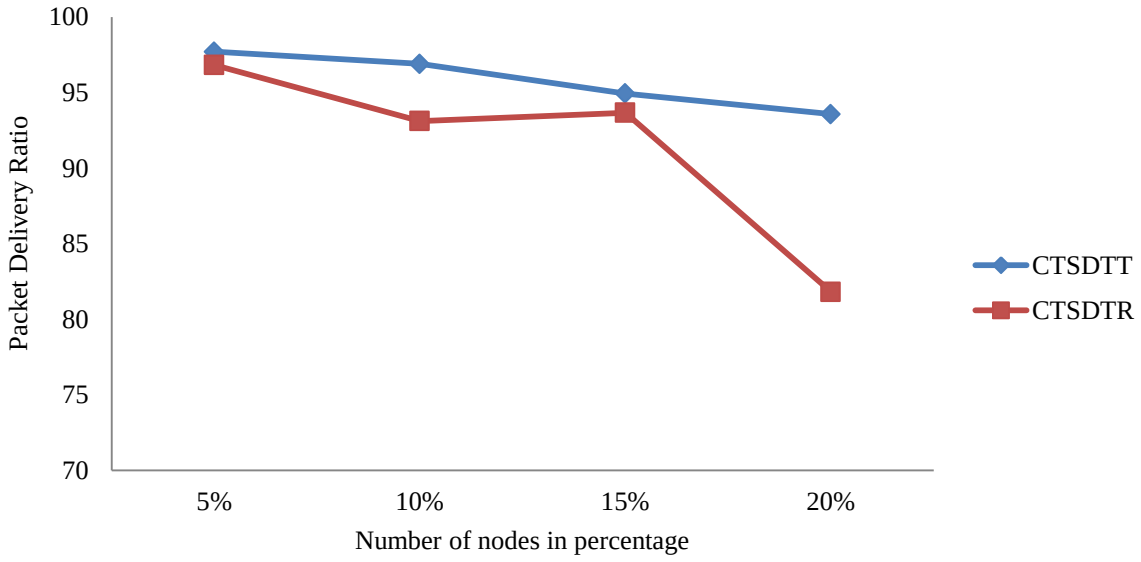


Fig. 6: Comparison of CTSDTT and CTSDTR based on packet delivery ratio by setting number of nodes in different percentage

PDR is defined as the ratio between the received packets by the destination and generated packets by the source. The calculation of packet delivery ratio is based on the received and generated packets as recorded in the trace file the Fig. 6 depicts the impact of designed security mechanism on delivery ratio. PDR lies between 0-100. The higher PDR means that the performance is high. In our experiments by considering different percentage of attacked nodes the performance of network is analyzed in terms of PDR against number of malicious nodes. The packet delivery ratio decreases when number of nodes increases in network. The CTSDTT has more packet delivery ratio than CTSDTR.

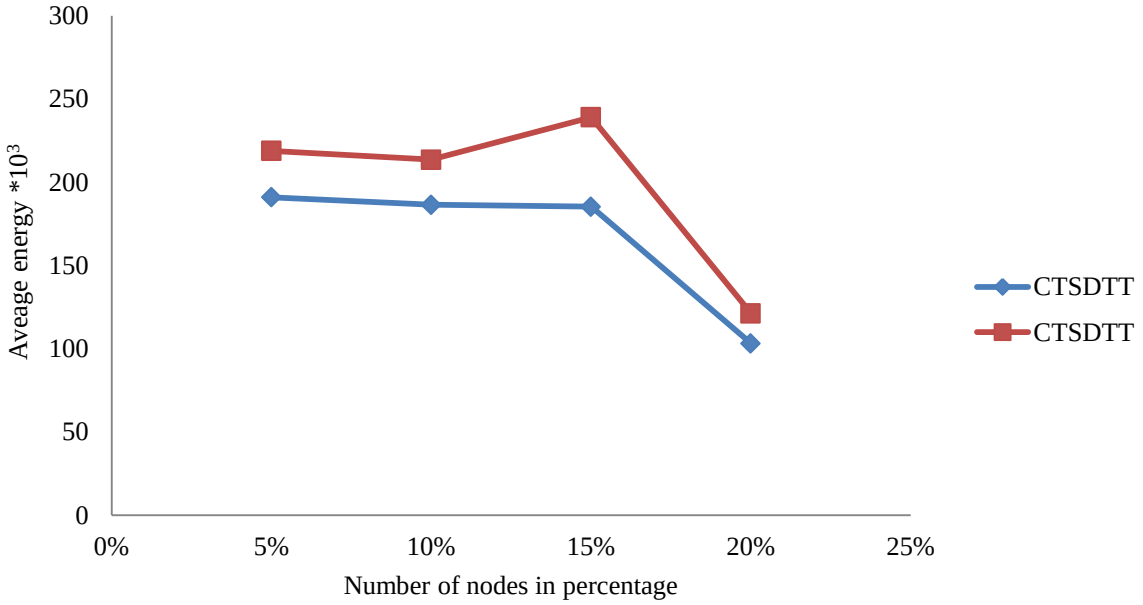


Fig. 7: Comparison of Average energy consumption for CTSDTT and CTSDTR.

Energy consumption is the amount of energy or power used in a process or system the Fig. 7: depicts the energy consumption. The analysis shows that energy consumption increases as number of nodes increases in network. The CTSDTT has less energy consumption than CTSDTR

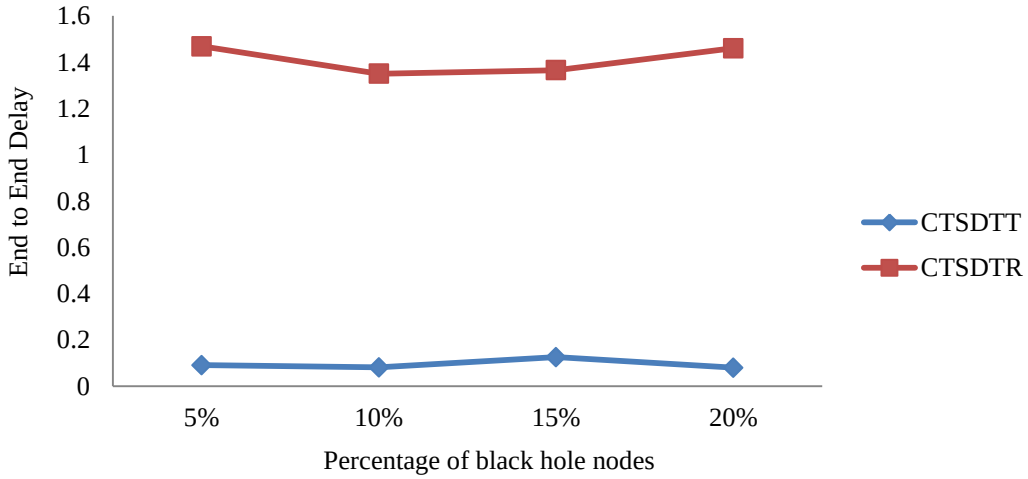


Fig. 8: Comparison of CTSDTT and CTSDTR in terms of end to end delay.

Delay is the difference between the time at which the sender generated the packets and the time at which the receiver received the packet. Delay is calculated using awk script which processes the trace file and produces the result. The Fig. 8 depicts that end to end delay is high in CTSDTR than CTSDTT.

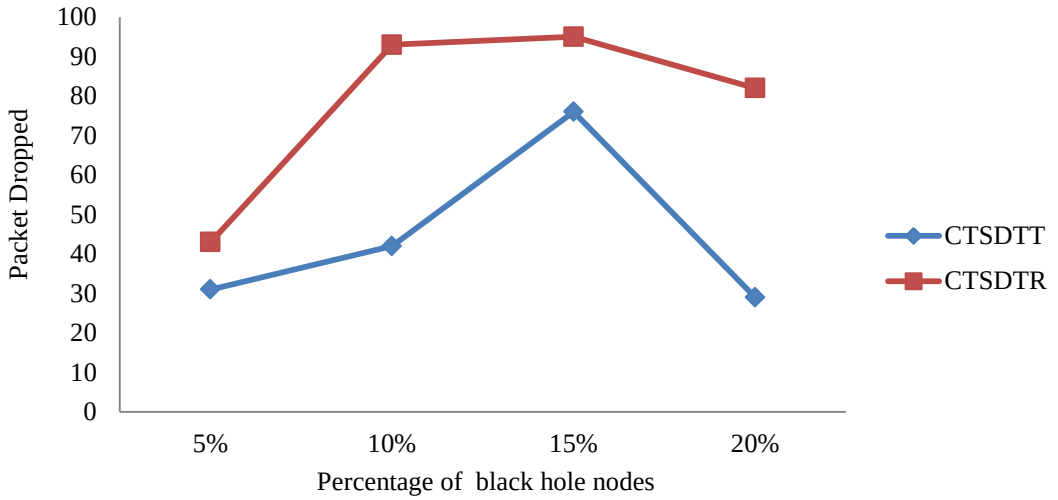


Fig. 9: Packet Dropped V/S Number of Nodes in Percentage for CTSDTT & CTSDTR

Packet loss in communication is difference between generated packets and received packets. Packet loss is calculated using awk script which processes the trace file and produces the result. The Fig. 9 shows the packets dropping in the network during data transmission. The figure depicts that data transmission using trust routing with Twofish encryption shows less packet dropping than the data transmission using RSA encryption.

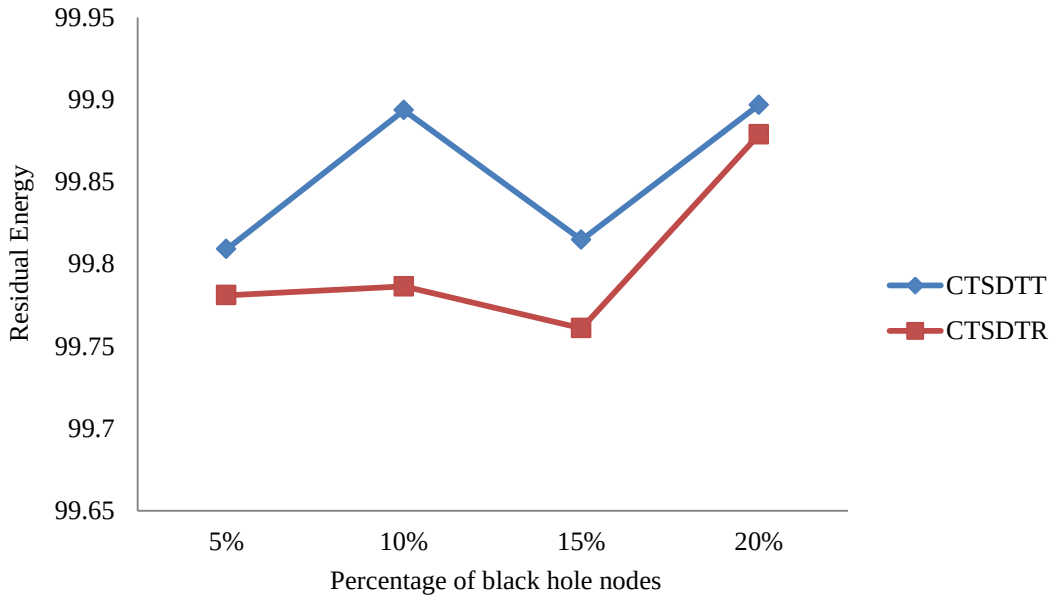


Fig 10: Residual Energy V/S Number of Nodes in Percentage for CTSDTT &CTSDR

Residual energy is the remaining energy after completion of the task the Fig. 10 shows that the residual Energy is high in CTSDTT than the CTSDTR.

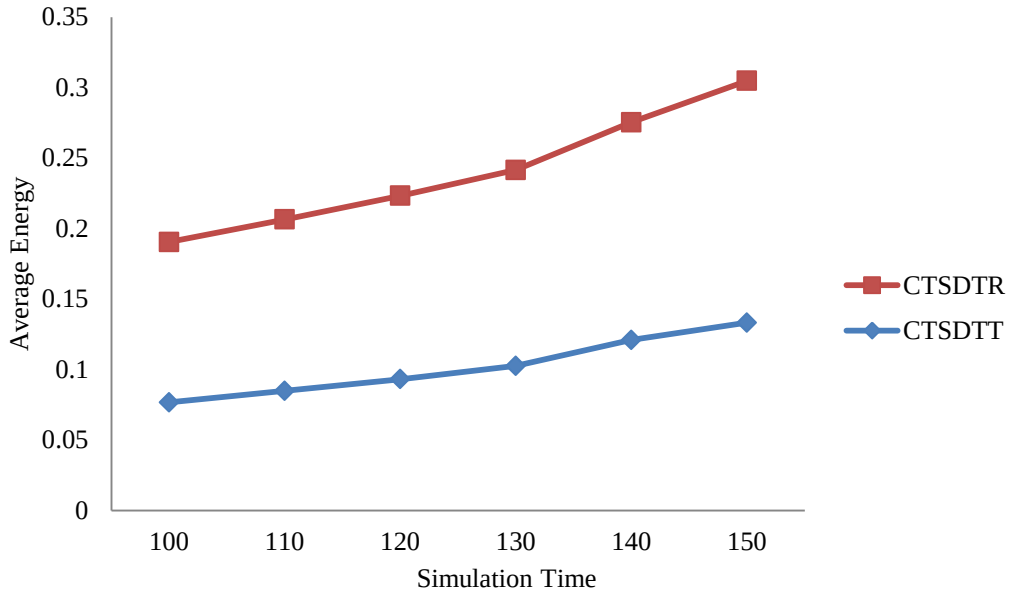


Fig. 11: Average Energy V/S Simulation Time for TCTSDT & RCTSDT

The Fig. 11 depicts that the average energy consumption for both CTSDTR and CTSDTT. Less energy consumption indicates that the performance of proposed work is high. It is measured in mille joules. The performance of proposed system is analyzed in terms of energy consumption against simulation time. The Twofish based secure data transmission consumes less energy compared to RSA based secure data transmission.

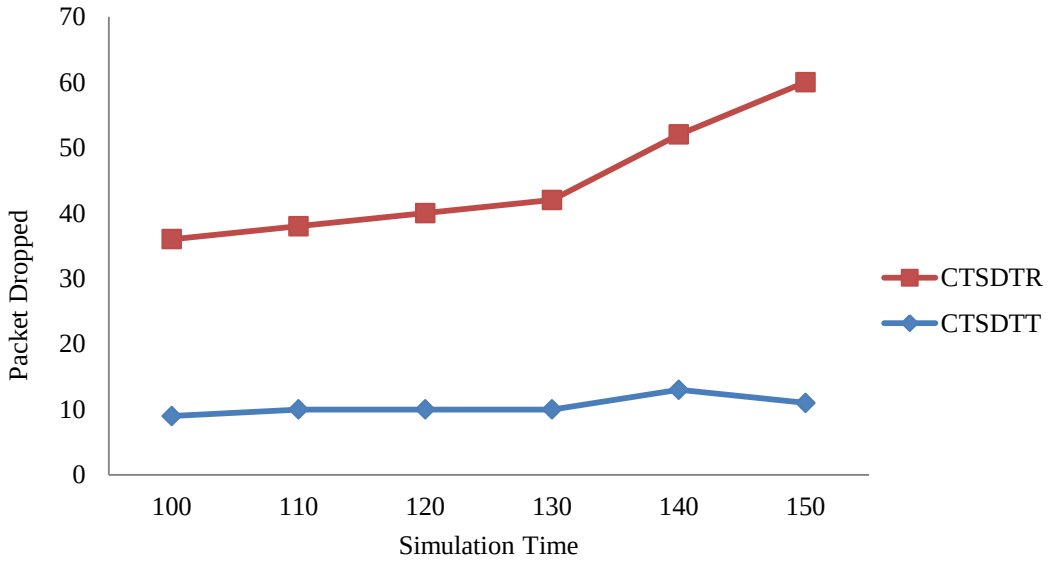


Fig. 12: Packet dropped V/S Simulation Time for CTSDTT & CTSDTR

From Fig. 12 it is clear that the packet dropping activity is less in Twofish based secure data transmission technique then the RSA. Less packet dropping during data transmission indicates that's the performance of network is good. The CTSDTT is showed less than 10% packet dropping in the network.

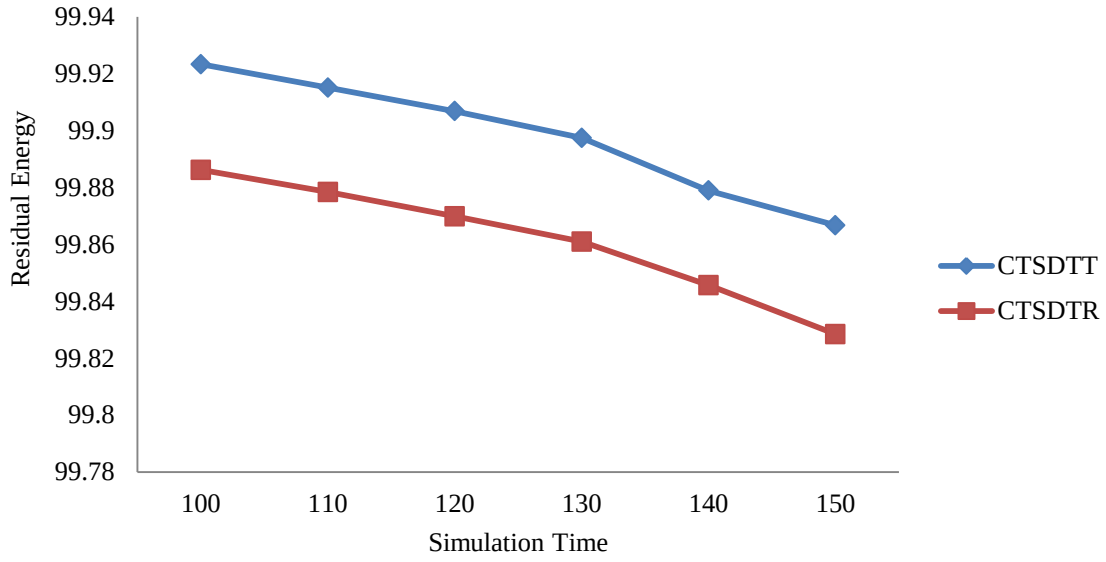


Fig. 13: Residual Energy V/S Simulation Time for CTSDTT & CTSDTR

The Fig. 13 shows that remaining energy after completion of task from assigned energy indicates that the energy consumed is less for Twofish based secure data transmission technique. And the residual energy is high for the initial simulation time, the residual energy decreases with the increased simulation time period for both the techniques.

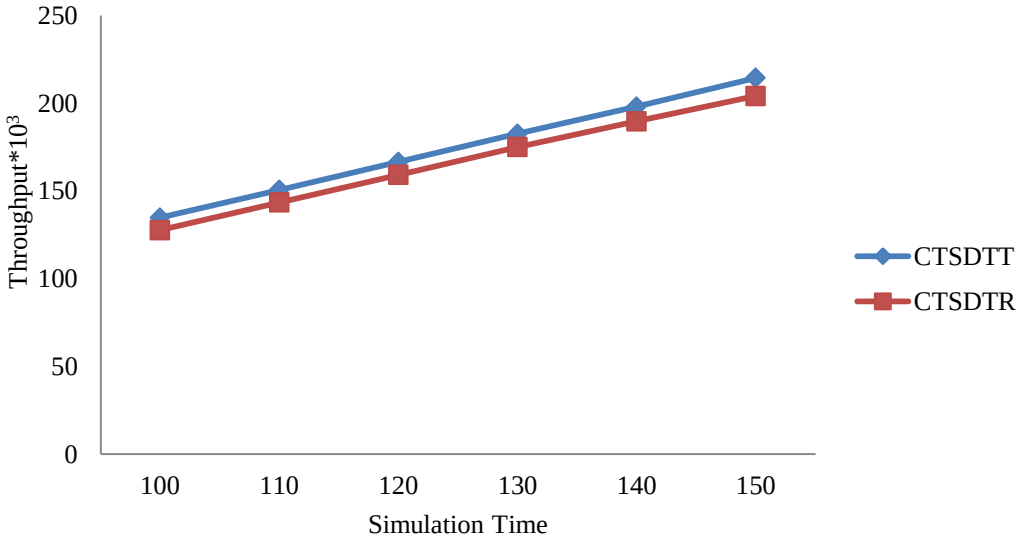


Fig. 14: Throughput V/S Simulation Time for CTSDTT & CTSDTR

The Fig. 14 shows throughput of the Twofish based secure data transmission and RSA based data transmission against simulation time. So it is clear that the throughput for Twofish is higher than the RSA.

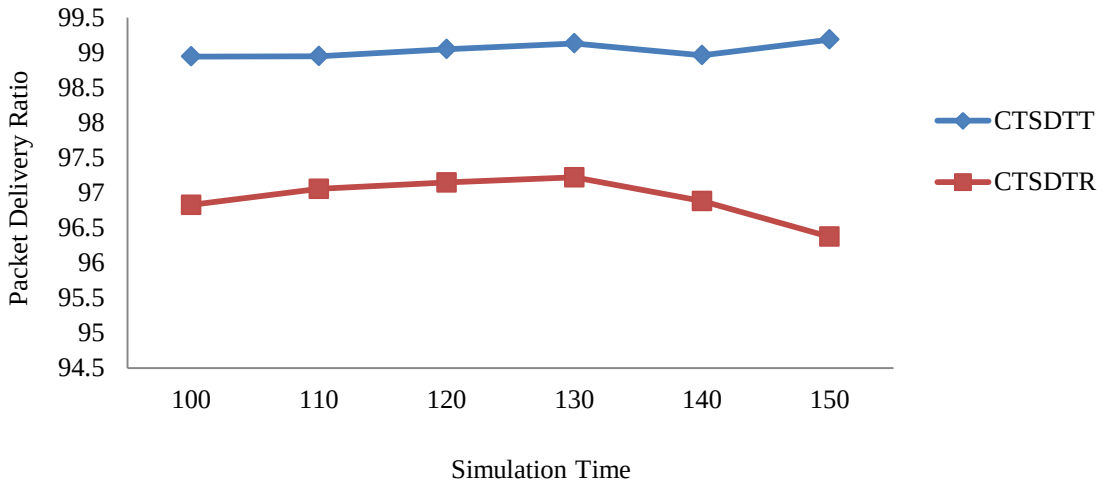


Fig. 15: Packet Delivery Ratio V/S Simulation Time for CTSDTT & CTSDTR

The packet delivery ratio against various simulation time is shown in Fig.15 from this it is clear that the proposed Twofish based secure data transmission technique is showing good performance in terms of PDR.

## VII. CONCLUSION

In order to provide security in the mobile ad hoc network the cryptography based design overlay is proposed. This paper presents improved algorithms for MANET networks. Data privacy is a vital problem in MANET networks these techniques are more secured due to encryption algorithms are used for secure data transmission. The designed protocol uses infrastructure nodes for detecting malicious node behavior in the network. The trust-based routing uses the trust value based on count of forwarded as message and received messages of each node for misbehavior detection. The cryptographic mechanism and infrastructure surveillance helps for providing a security service in the network. The algorithms RSA and Twofish for security feature are implemented and made comparison of performance of these algorithms and proved that the Twofish algorithm is easy and efficient with improved performance.

## REFERENCES

[1] Mohamed A. Abdelshafy, Peter J. B. King “Resisting blackhole attacks on MANETs”, IEEE, 2016, pp.1048-1053.

[2] S Tan, P Sok, K kin “Using cryptographic technique for secure route discovery and data transmission from blackhole attack”,international journal of network, cited by 2, 2014.

[3] Juhi Biswas, Ajay Gupta, Dayashankar singh, “WADP: A Wormhole Attack Detection And Prevention Technique in MANET using Modified AODV routing protocol”, IEEE ,2014, pp.1-6.

[4] S. R. Meddi, Muralidhar Meddi, Sireesh Gavini “Detecting Packet-dropping in MANET”, IEEE, vol. 42, 2012, pp. 0975 – 8887.

[5] Shubh Lakshmi Agrwal, Rakhi Khandelwal, Pankaj Sharma "Analysis osf detection algorithm of Sinkhole attack & QoS on AODV for MANET", IEEE (NGCT), 2016, pp.839-842.

[6] U. Pandey, M. Manoria, and J. Jain, "A novel approach for image encryption by new m box encryption algorithm using block based transformation along with shuffle operation." International Journal of Computer Applications, 42(1), 2012.

[7] Pranjali Deepak Nikam, Vanita Raut, "Improved MANET Security Using Elliptic Curve Cryptography and EAACK", IEEE (ICCN), 2015, pp.1125 – 1129.

[8] A. Kumar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, July 2012.

[9] C, E perkins, E.M. royer, "Adhoc-on-demand distance vector routing", IEEE, 1999, pp. 90-100.

[10] Rubeena Jabi , Punyaban, Deepty Dubey , "An efficient secure data transmission based on visual cryptography", IEEE, 2016 ,pp.1-6.

[11] L. Rubun Qinghua, Z. Sencun, and C. Guohong, "Routing in socially selfish delay tolerant networks", IEEE, infocom, 2010, pp. 1-9.

[12] W. Sherchan, S. Nepal, and C.paris, "A survey of trust in social networks", ACM comput. Surveys, vol 45, no. 4, Aug. 2013, Art. No.47.

[13] Muhammad Saleem Khan, Danile Mide, Majid.I.Khan, Elisa Bertino "Adaptive Trust Threshold Strategy for Misbehaving Node Detection and Isolation", IEEE, 2015, pp.718-725.

[14]Ying Zhu, Bin Xu, et al. "A Survey of Social Based Routing in Delay Tolerant Networks: Positive and Negative Social Effects ", IEEE, 2013, vol 15, pp. 387-401.

[15] Imad Jawhar, Farhan Mohammed, Jammela Al Jaroodi and Nader mohamed "TRAS: A Trust-Based Routing Protocol for Ad Hoc and Sensor Networks", IEEE, 2016, pp. 382-387.