International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

H-EAACK-An Intrusion Detection System Using Hybrid Cryptography for MANET

Randeep Kaur Kahlon[1], Dr.J.W.Bakal[2]

[1]*Assistant Professor, Terna Engineering College,Nerul,Navi Mumbai, Maharashtra.*
[2]*Principal, Shivajirao Jondhale College Of Engineering, Dombivli, Thane, Maharashtra.*

Abstract - *The migration to wireless network from wired network has been adopted in the past few decades. MANET, mobile ad-hoc network is one of the most important applications of wireless network. MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. MANETs are used in applications like military and in natural disasters. Security measures play an important role in all these applications .Hence it is necessary to include intrusion-detection system for MANETs. There are various IDS proposed by researchers. One of them is EAACK (Enhanced Adaptive Acknowledgement) which demonstrates higher malicious behavior detection rates while does not greatly affect the network performances. EAACK scheme has used digital signatures for authentication process. All the acknowledgements are digitally signed. EAACK worked by implementing both DSA and RSA algorithm. But EAACK does not provide encryption to the data packets. It causes the network overhead when the malicious nodes are increased. To improve EAACK, we propose a hybrid cryptography scheme which uses symmetric as well as asymmetric cryptographic techniques. Hybrid scheme is implemented using symmetric cipher Triple DES and public key cryptography RSA with hash function MD5. The Triple DES algorithm provides confidentiality, the hash function provides the integrity and RSA will ensure the authentication.*

Key Words: **RSA, DSA, EAACK, IDS,TWOACK, ACK, AACK**

1.INTRODUCTION

1.1 MANET

A mobile ad-hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Wireless links make MANET more susceptible to attacks. This violates the networks goals of availability, integrity, authentication, and no repudiation. There are two types of MANET: closed and open. In a closed MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/ rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity.

1.2 Intrusion Detection System (IDS)

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. An IDS is software that facilitates the intrusion detection process, initial responsibility of IDS is to detect undesirable and intruder activities. It is the defensive mechanism in the mobile ad hoc network which provides the secured communication in between the nodes.

1.3 Hybrid Cryptography

Cryptography is the study of techniques for secure communication in the presence of third parties. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. A hybrid cryptosystem can be constructed using any two separate cryptosystems:

- key encapsulation scheme, which is a public-key cryptosystem, and
- data encapsulation scheme, which is a symmetric-key cryptosystem.

2. RELATED WORK

Marti, Giuli, Lai and Baker [1] described the two techniques that increase the throughput in the presence of nodes that agree to forward the packets but fail to do so. The techniques are Watchdog and Pathrater. In watchdog, suppose S send data to D, then all the intermediate nodes stores packets in the buffer. If the packet remains with the node more than the timeout value then failure tally is incremented by Watchdog. Then if the failure tally increases than the threshold value then Watchdog detects node as malicious node and sends message to the source. Watchdog increases the throughput of network to 27% but increases the network overhead to 24% from 17%. Watchdog identifies the misbehaving nodes and Pathrater avoids the

routing through these nodes. Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; and 6) partial dropping.

To overcome the weakness of Watchdog and Pathrater, Nasser and Chen introduced intrusion detection system called ExWatchdog [2]. Through overhearing, each node can detect the malicious action of its neighbors and report other nodes. However, if the node that is overhearing and reporting itself is malicious, then it can cause serious impact on network performance. The main concern here was to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Routeguard assigns ratings to nodes and calculates a path metric in a refined way. If the real malicious node is on all paths from specific source and destination, then it is impossible for the source node to confirm with the destination of the correctness of the report. It decreases network overhead. Parker [3] presents network intrusion detection mechanisms that uses snooping algorithm to detect misbehavior in the mobile adhoc networks. Two response mechanisms are used - Passive to detect if node is intrusive and protects itself from attacks and Active to detect if node is intrusive and act to protect all nodes from attacks. A mis-route cannot be determined but any modification and packet dropping can be identified and locked.

TWOACK proposed by Liu et al. [4] is neither an enhancement nor a Watchdog-based scheme. TWOACK detects misbehaving links by acknowledging every data packet trans-mitted over every three consecutive nodes along the path from the source to the destination. Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR). Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious. The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. The acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead.

Based on TWOACK, Sheltami et al. [5] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be considered as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet. They fail to detect malicious nodes with the presence of false misbehaviour report and forged acknowledgment packets.

To remove maximum problem of watchdog which cannot be solved by previous methods the new Enhanced AACK (EAACK) scheme [6] is developed and evaluated through implementation. It solves four significant problems of Watchdog mechanism, which are ambiguous collisions, receiver collisions, limited transmission power and false misbehavior report. It detects the malicious nodes by verifying ACK packets. Security is not provided over here for ACK packets. Hence, there is possibility that ACK packet is misused or not send from intended receiver. EAACK suffers from the threat that it fails to detect misbehaving node when the attackers are smart enough to forge the acknowledgement packets. Hence, Sheltami [7] introduced Digital Signature Algorithm (DSA) into the EAACK scheme, and investigate the performance of DSA in MANET. The purpose of this paper is to present an improved version of EAACK called EAACK2 that performs better in the presence of false misbehavior and partial dropping.

Sheltami[8] introduced Digital Signature Algorithm (DSA) and RSA both into the EAACK scheme, and investigated the performance of DSA as well as RSA in MANET. They arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. It reduces network overhead.

The threats an ad hoc network faces and the security goals to be achieved must be considered. It should focus on how to secure routing and how to establish a secure key management in an ad hoc networking environment. To build a highly available and highly secure key management service, threshold cryptography [9] has been proposed to distribute trust among a set of servers. AODV is also considered in detail and developed a security mechanism to protect its routing information [10]. The Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [11], a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial of- Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, it used efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. Bandwidth and power constraints are the important factors to be considered in current wireless network because multi-hop ad-hoc wireless relies on each node in the network to act as a router and packet forwarder [12]. This dependency places bandwidth, power computation demands on mobile host to be taken into account while choosing the protocol.

3. IDS FOR MANET

In this section, we will study all proposed IDS schemes in detail.

3.1 WATCHDOG

Marti et al. [1] proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. Suppose there exists a path from node S to D through intermediate nodes A, B and C. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. Figure 1 illustrates how the watchdog works. When B forwards a packet from S towards D through C, A can overhear Bs transmission and can verify that B has attempted to pass the packet to C. The solid line represents the intended direction of the packet sent by B to C, while the dashed line indicates that A is within transmission range of B and can overhear the packet transfer.

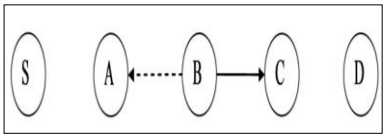

Fig -1: Working of watchdog.

3.2 TWOACK

The working process of TWOACK is shown in Figure 2. Node A first forwards Packet 1 to node B, and then, node B forwards Packet 1 to node C. When node C receives Packet 1, as it is two hops away from node A, node C is obliged to generate a TWOACK packet, which contains reverse route from node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from node A to node C is successful. Otherwise, if this TWOACK packet is not received in a predefined time period, both nodes B and C are reported malicious.

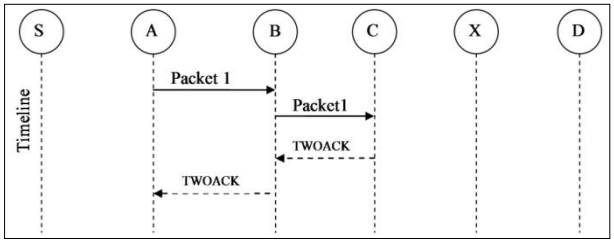

Fig -2: TWOACK scheme.

The same process applies to every three consecutive nodes along the rest of the route.

3.3 AACK

Based on TWOACK, Sheltami et al. [5] proposed a new scheme called AACK. In the ACK scheme shown in Figure7, the destination node is required to send back an acknowledgment packet to the source node when it receives a new packet, the source node S sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet. When the destination node D receives Packet 1, it is required to send back an ACK acknowledgment packet to the source node S along the reverse order of the same route. Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TACK scheme by sending out a TACK packet.

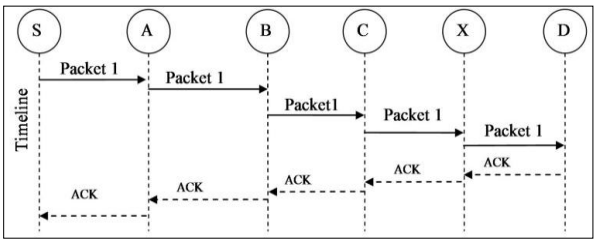

Fig -3: AACK Scheme

3.4 EAACK

To remove maximum problem of watchdog which cannot be solved by previous methods the new Enhanced AACK (EAACK) scheme is developed and evaluated through implementation [6]. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehaviour report authentication (MRA).

1. ACK

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. Within a predefined time period, if node S receives Packet, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK data packet to detect the misbehaving nodes in the route.

2. S-ACK

The S-ACK scheme is an improved version of the TWOACK scheme proposed by Liu et al. [4]. The principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode was to detect misbehaving nodes in the presence of ambiguous collision, receiver collision or limited transmission power.

3. MRA

The MRA scheme is designed to resolve the weakness of Watchdog when it fails to detect misbehaving nodes with the presence of false misbehavior report. The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. This attack can be fatal to the entire network when the attackers break down sufficient nodes and thus cause a network division. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through different route.

4. PROPOSED METHODOLOGY

EAACK demonstrates higher malicious behavior detection rates in certain circumstances while does not greatly affect the network performances. The functions of intrusion detection schemes all largely depend on the acknowledgment packets. Hence, it is crucial to guarantee that the acknowledgment packets are valid and authentic. To address this concern, we adopted a digital signature in scheme named Enhanced AACK (EAACK). The data packets are not encrypted in the transmission from source to destination. The authenticity, integrity and confidentiality are the most important concerns of the security. To address all the above concerns and improve security in existing EAACK scheme, we propose hybrid cryptography techniques in the existing scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be encrypted using the hybrid encryption scheme before they are sent out and verified for their integrity until they are accepted.

The proposed system comprises the following modules:

1. **EAACK**
   - Acknowledgement (ACK).
   - S-Acknowledgement (S-ACK).
   - Misbehavior Report Authentication (MRA).
2. **HYBRID ENCRYPTION AND DECRYPTION**

4.1 EAACK (Enhanced Adaptive Acknowledgement)

EAACK process is shown in Fig. 4, Source node (S) sends data packet to destination node (D) and if it receives the data packet, it sends an ACK back to node A in the reverse order. Within a predefined time period, if node S receives the ACK, then the packet transmission from node S to node D is successful. Otherwise it switches to S-ACK mode. In S-ACK mode, for every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. If first node does not receive this acknowledgment packet within a predefined time period, both nodes second and third are reported as malicious. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. The MRA scheme is designed detect misbehaving nodes with the presence of false misbehaviour report. In MRA mode the source node tries to find an alternate path to the destination node and it sends an MRA packet along this route to circumvent the misbehaviour reporter node. When the destination node receives the MRA packet it checks whether it has received the reported packet. If it is already received, then it is a false misbehaviour report and whoever generated this report is marked as malicious. Otherwise, the misbehaviour report is trusted and accepted.

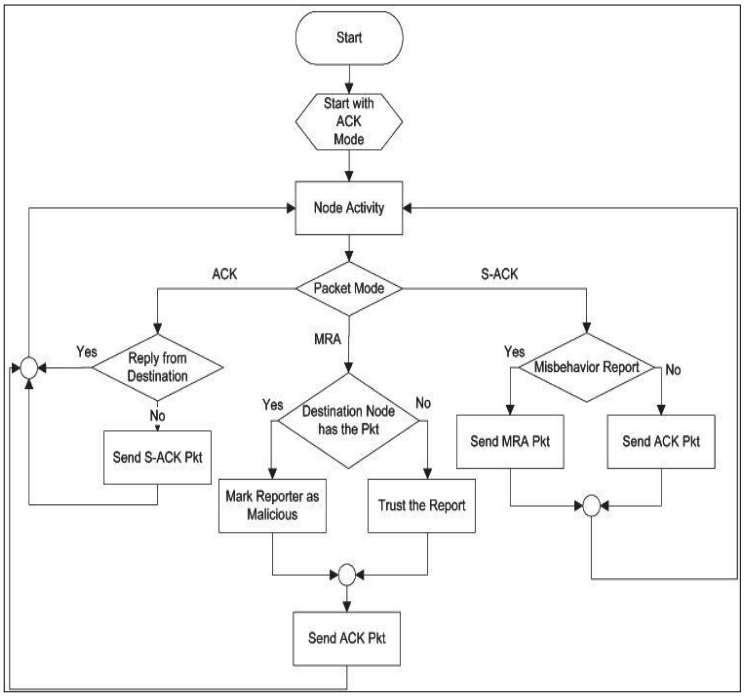

Fig-4:EAACK Flow

4.2 HYBRID ENCRYPTION AND DECRYPTION

Encryption Process

1. MD5 algorithm computes 128 Bit MD5.
2. Reduce 128-bit message digest to 112 bits by discarding every number that is a multiple of 8-bit used for parity. This output is called as MD'.
3. Triple DES algorithm encrypts the Original Message (M) with help of MD' as symmetric key used in triple DES, and then produce a cipher text (CT).
4. The MD' Encrypted by RSA Algorithm with receiver Public key BPK and produce Cipher Text of Key (CK).
5. Combine a Cipher Text (CT) and Cipher text of Key (CK), produces a Complex Message (CM).Complex Message (CM) is sent to the Receiver B.

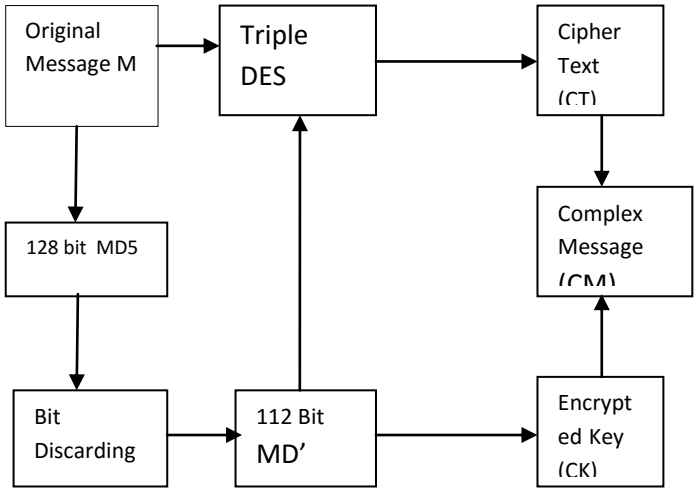

Fig-5: Hybrid Encryption

Decryption Process:
1. The receiver B received cipher text CT into two parts, one is cipher text of key CK from the RSA algorithm encryption, and the other is cipher text CT from the triple DES algorithm encryption.
2. The receiver B decrypts cipher text of key CK by their own private key BSK, and retrieve the key K, then decrypt the cipher text CT to the original M by key K that is MD'.

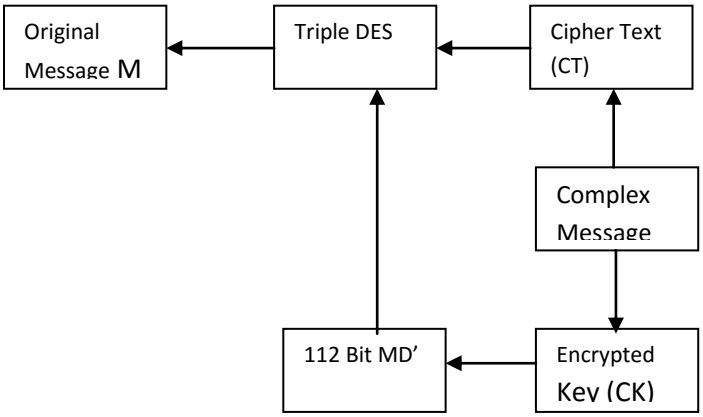

Fig-6: Hybrid Decryption

5. RESULTS AND DISCUSSIONS

Our simulation is conducted within the Network Simulator (NS) 2.34 environment. The system is running on a laptop with Core 2 Duo T7250 CPU and 3-GB RAM. In order to better compare our simulation results with other research works, we adopted the default scenario settings in NS 2.34. In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics:
1) Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.
2) Packet Loss: The packet loss is the total number of packets lost during the entire transmission of data across the network.
3) Delay**:** The delay is defined as the time required by the transmission packets to reach destination.

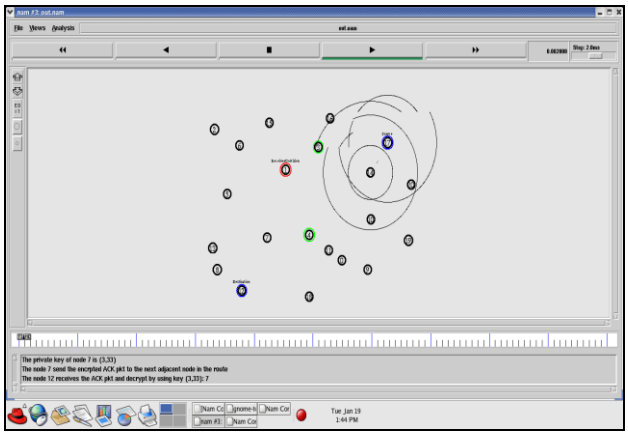

Fig-7: Node data transmission takes place using EAACK.
The Node data transmission using EAACK Method is shown in Figure 7.
The hybrid encryptiuon and decryption part is implemented in Java Platform as it is worth implementing in real-time. Its Process is shown in Figure 8.

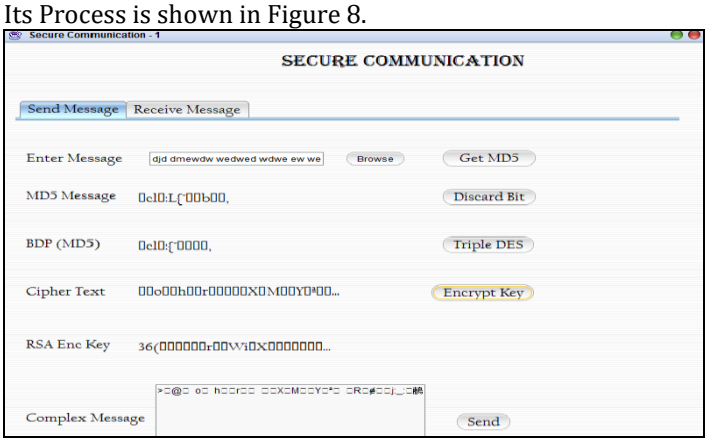

Fig-8: Hybrid encryptiuon and decryption

1) Packet Delivery Ratio (PDR)

The PDR for the EAACK implemented is shown in Figure 9.

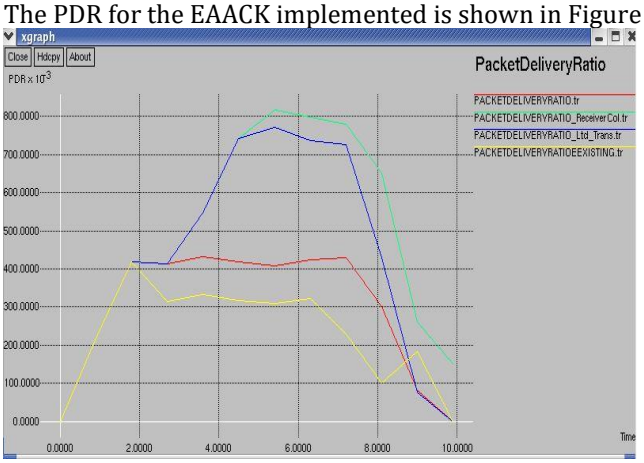

Fig-9: PDR

2) Packet Loss

The loss of packets for the EAACK implemented is shown in Figure 10.

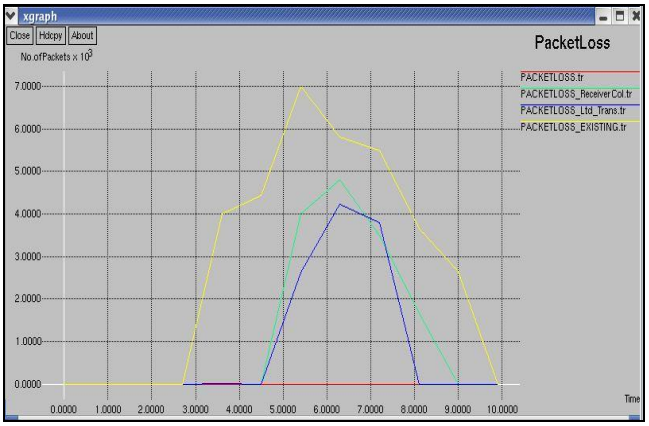

Fig-10: Packet Loss

3) Delay

The delay of EAACK implemented is shown in Figure 11.

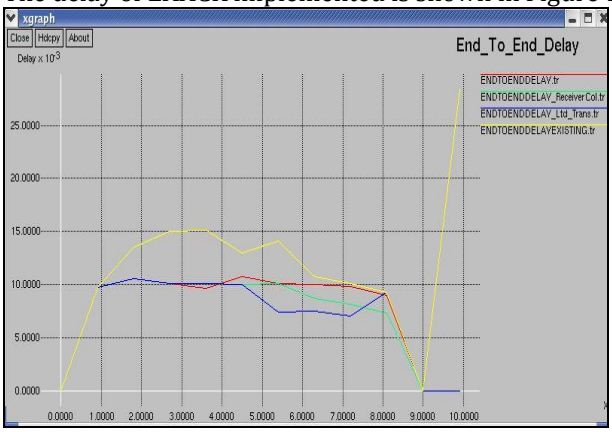

Fig-11: Delay

Hybrid Encryption and Decryption module performance is measured in terms of encryption and decyption time. The results of encryption and decryption times of various files of different sizes are shown in table I and Figure 12 respectively.

Table -1: Plain Text file size with Encryption and Decryption Time

File type (Text File In Bytes)	Encryption time (ms)	Decryption Time (ms)
40 Bytes	1200	670
81 Bytes	530	470
300 Bytes	430	550
1613 Bytes	715	797

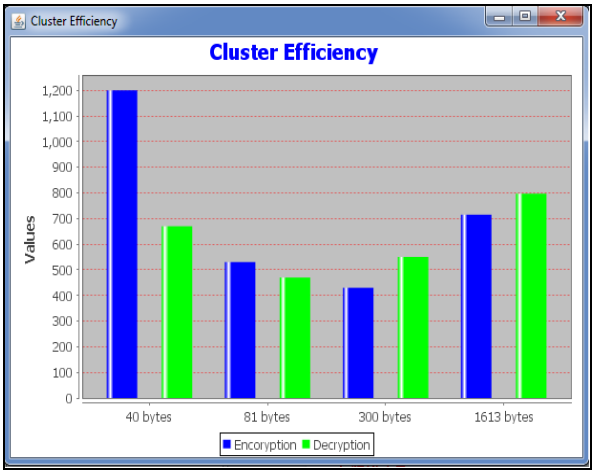

Fig-12: Graph of time for different file sizes

3. CONCLUSIONS

Packet-dropping attack has always been a major threat to the security in MANETs. In our proposed system, we have introduced a novel IDS named Intrusion detection system using hybrid cryptography specially designed for MANETs and will compare it against existing mechanism in different scenarios through simulations. The problems of receiver collision, limited transmission power, and false misbehavior have been eliminated. To prevent the attackers from initiating forged acknowledgment attacks, the proposed system implements the hybrid cryptography concept in order to improve security. It improves the network's PDR when the attackers are smart enough to forge acknowledgment packets. Using hybrid encryption scheme we can improve confidentiality, availability and integrity of the system. So our proposed system ensures more security to the network and also improves throughput.

REFERENCES

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

[2] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf.Perform., Comput., Commun.*, 2004, pp. 747–752.

[3] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network," in *Proc. IEEE Int. Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, —An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs‖, IEEE Transactions on Mobile Computing, May 2007.

[5] Al-Roubaiey, A.; Sheltami, T.; Mahmoud, A.; Shakshuki, E.; Mouftah, H., "AACK: Adaptive Acknowledgment Intrusion

Detection for MANET with Node Detection Enhancement," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.634-640, 20-23April2010.
[6] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10, 2010, pp. 216–222.
[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis,Singapore, Mar. 22–25, 2011, pp. 488–494.
[8] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami —EAACK—A Secure Intrusion-Detection System for MANETs, IEEE Transactions on Industrial Electronics, Vol. 60, No 3, March 2013.
[9] L. Zhou and Z. Haas, "Securing ad-hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[10] M. Zapata and N. Asokan, "Securing *ad hoc* routing protocols," in *Proc. ACM Workshop Wireless Secur.*, 2002, pp. 1–10.
[11] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.
[12] R. Rivest, A. Shamir, and L. Adleman, —A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, vol. 21, no. 2,Feb. 1983, pp. 120–126.
[13] Botan, A Friendly C ++ Crypto Library. [Online]. Available: http:// botan.randombit.net/