Removal of Malicious Attacks using Hybrid Symmetric Cryptograhic Technique

V. Umadevi
Research Scholar,
Computer Science Department, Karpagam
University, Coimbatore, 642120, India

C. Chandrasekar
Associate Professor,
Computer Science Department,
Periyar University, Salem, 636011, India

ABSTRACT

Security in Mobile Ad-hoc Network (MANET) plays an important role for providing effective network service without any malicious attack. Intrusion detection is crucial in improving the performance of mobile ad-hoc network. Intrusion detection monitors the activities in a mobile system by collecting the information and then analyzing them. Most previous works for intrusion detection use the current acknowledgement and location-based routing protocol to combat against the intrusion detection. In this work to secure the mobile network system from malicious attacks, Hybrid Symmetric Cryptography Technique (HSCT) is introduced. The HSCT uses Advanced Encryption Standard (AES) and Message Digest 5 (MD5). Advanced Encryption Standard (AES) is based on the principle of substitution and permutation keying model adapted as node ids in the mobile ad-hoc network. AES ensures higher amount of packets being transmitted with minimum packet delay. The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words in mobile nodes to remove the malicious attack. AES and MD5 fused together on the mobile nodes to communicate packets with high security. The HSCT algorithms offer data security and users authenticity using a mixture of two symmetric cryptographic techniques. HSCT measure and analyze different parameters such as true positive rate on detecting abnormal activities, packet delay, rate of intrusion being detected with respect to node density and packets being transmitted. The HSCT is simulated using NS2. Experiment results show that the proposed technique achieves better performance in considerably minimizing the packet delay rate by 33.36% and improves the true positive rate on detecting abnormal activities by 25.83% compared to the state-of-the-art works.

Keywords

MANET, Intrusion detection, Location-based routing protocol, Symmetric Cryptography, Advanced Encryption Standard, Message Digest

1. INTRODUCTION

Intrusion detection monitors the activities in a mobile system by collecting the information and then analyzing them. The intrusion detected work establishes the activities and once IDS determine an unusual activity, then that is known to be an attack. Many researchers have contributed in the field of intrusion detection.

A new intrusion detection system called, Enhanced Adaptive ACKnowledgement (EAACK) [1] designed mechanism to protect MANET from attacks using digital signature resulting in the improvement of packet delivery ratio and reducing the routing overhead. Anonymous Location-Based Efficient Routing Protocol (ALERT) [2] provided anonymity protection to sources, destination and routes through counter intersection strategy. Though intrusion detection was efficiently monitored, but authentication was compromised. To ensure authentication, Partially Observable Markov Decision Process (PODMDP) [3] was designed using structuring of multi-armed bandit problem.

A black hole attack on a MANET forcibly obtains the route from a source to a destination by falsifying the sequence number and hop count of routing. Anti Black Hole (ABH) [4] mechanism was designed with the objective of minimizing the false positive by appropriating the threshold set. Another anti collision protocol [5] for Radio Frequency-based Identification (RFID) was designed to measure the collision level with time system efficiency using group of tags. Combating the attack by preserving the location details was presented in [6] using sink simulation and backbone flooding. Another authentication-based model to secure against all the attacks was presented in [7] using cryptographic methods.

Mobile Ad-hoc NETworks (MANETs) have received significant attention due to the multi hop nature and infrastructure-less transmission. However, due to the error prone channel and dynamic changes in network topology, ensuring reliable data delivery in MANETs has posed serious problems. Position-based Opportunistic Routing (POR) [8] protocol was designed to reduce the latency by local route recovery using Virtual Destination-based Void Handling (VDVH) scheme.

Cooperative defense against collusion attack was designed in [9] using SpaceMac. A novel homomorphic MAC scheme was introduced reducing the computation and communication overhead. In [10], optimal jamming attack strategies and defense policies were introduced aiming at minimizing the attack rate through heuristic technique. Avoiding attacks through congestion control was designed in [11] based on round trip time.

Today’s location-sensitive applications highly depend on the mobile device of the user’s in determining the current location. This in turn provided access to malicious by providing bogus alibis by cheating on their locations. In [12], A Privacy Preservation Location Proof Updating System (APPLAUSE) to detect the colluding attacks was presented. Measures were taken to reduce the Vampire attack [13] using proof of concept protocol. Keying mechanism based on Virtual Energy Based Encryption and Keying (VEBEK) [14] was designed aiming at eliminating malicious data. In [15] a framework for intrusion detection in IEEE 802.11 was designed for investigating the intrusion detection systems. Proactive mechanisms to handle black hole attack [16] using timely mandate and hole detection procedure was designed.

An intrusion detection system (IDS) node selection method based on assignment algorithm was designed in [17]. This method also ensured network lifetime. A review of intrusion detection systems was presented in [18]. However, security issues were not solved. To solve the security issues involved in MANET, in [19], the most common threats to ad hoc network was presented and measures to alleviate was also discussed. Intrusion detection model for Optimized Link State Routing (OLSR) protocol was designed in [20].

In this paper, a novel Hybrid Symmetric Cryptography Technique (HSCT) is proposed, in which AES and MD5 is fused together on mobile nodes that communicate the data packets in a significant manner ensuring higher amount of security. The contributions of HSCT are summarized as follows. This paper propose a Substitution and Permutation-based Advanced Encryption Standard (SP-AES) which can be deployed without complex modification in MANET and achieve packet transmission rate. The concept of key generation and rounding function in SP-AES model significantly enhances the robustness of the data packets transmission and reduces the packet delay time. In the case of removing the malicious attack, we propose a MD5-based malicious attack removal process in which the advantages of true positive rate on abnormal activities are ensured. Finally, we evaluate the performance of HSCT through extensive simulations and verify that HSCT achieves excellent performance in the face of high node mobility ensuring security.

The rest of the paper is organized as follows. Section 2 presents an overview of the malicious attack removal technique proposed, and presents a new analysis of each in terms of their true positive rate on detecting abnormal activities. Section 3 describes the experimental settings through parametric settings used for conducting the experiments in NS2. Section 6 discuss the results of an ns2-based performance evaluation of HSCT and other major representatives of the Enhanced Adaptive ACKnowledgement (EAACK) [1] and Anonymous Location-Based Efficient Routing Protocol (ALERT) [2] in MANET. Finally, Section 7 concludes the paper.

2. HYBRID SYMMETRIC CRYPTOGRAPHY TECHNIQUE

This section describe the proposed Hybrid Symmetric Cryptography Technique in detail. The technique described in this work is based on the previous work [1] [2], where the backbone of secure intrusion detection system for MANET was proposed and evaluated through implementation. This paper extend it with the introduction of Hybrid Symmetric Cryptography Technique to perfectly secure the mobile network system from malicious attacks. The Hybrid Symmetric Cryptography Technique consists of two main parts, namely Substitution and Permutation-based Advanced Encryption Standard and MD5 algorithm.

2.1 Substitution and Permutation-based Advanced Encryption Standard

Substitution and Permutation-based Advanced Encryption Standard (SP-AES) in HSCT is a symmetric block cipher based on the principle of substitution and permutation keying model adapted as node ids in the mobile ad-hoc network. While sharing the data packets between mobile nodes in network, security accomplishment is performed. The HSCT uses the SP-AES aiming at improving the packet transmission rate significantly. The SP-AES processes data packets with a fixed block size of with three key sizes of 128, 192 or 256 bits.

AES function on a '$4 * 4$' column order matrix which computes down on the predetermined network field. The operations of '$4 * 4$' column order matrix are performed on the State. The state represents a two-dimensional array of bytes that includes the Plaintext that comprises of four rows and four columns. Similarly, the Key Schedule is represented in the form of a two-dimensional array which contains the Key. Figure 1 shows the structure of SP-AES model followed in HSCT.

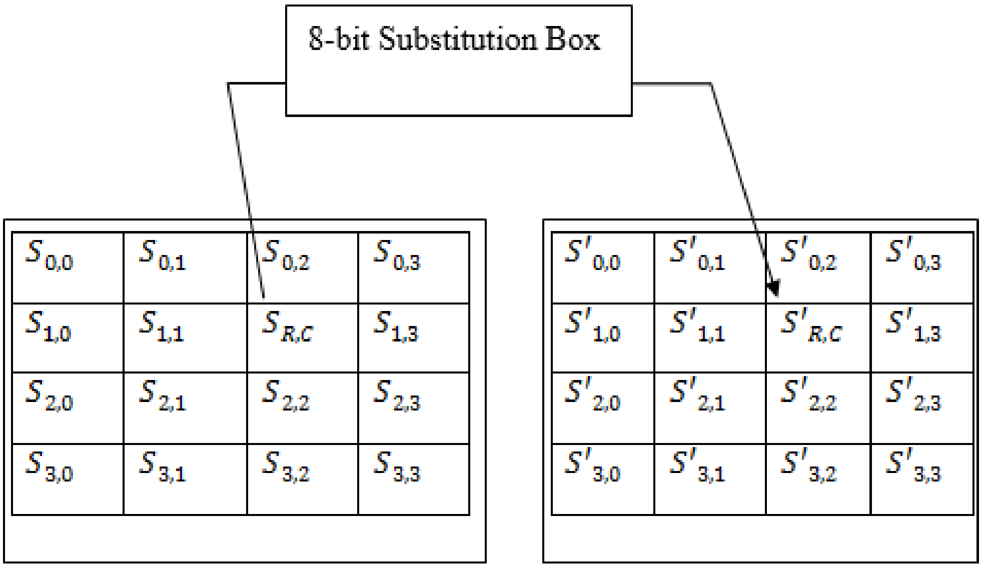
8-bit Substitution Box
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{R,C}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$ $S_{2,2}$ $S_{2,3}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S'_{0,0}$ $S'_{0,1}$ $S'_{0,2}$ $S'_{0,3}$
$S'_{1,0}$ $S'_{1,1}$ $S'_{R,C}$ $S'_{1,3}$
$S'_{2,0}$ $S'_{2,1}$ $S'_{2,2}$ $S'_{2,3}$
$S'_{3,0}$ $S'_{3,1}$ $S'_{3,2}$ $S'_{3,3}$

Figure 1 Structure of 8-bit 4 * 4 Substitution Box

Whenever a node (i.e. $MN_i = MN_1, MN_2, \dots, MN_n$) has to send the data packets (i.e. $DP_i = DP_1, DP_2, \dots, DP_n$) to the other node (i.e. destination node DN), the cipher operation is performed. At this juncture, the input Plaintext is copied to the State whereas the input Key is copied to the Key Schedule. The input key for SP-AES model specifies the number of repetitions that convert plaintext, into the final ciphertext, where the cycles of repetition are formulated as below.

$$\boldsymbol{Cycles_r = 10\ for\ 128 - bit} \quad \textbf{(1)}$$

$$\boldsymbol{Cycles_r = 12\ for\ 192 - bit} \quad \textbf{(2)}$$

$$\boldsymbol{Cycles_r = 14\ for\ 256 - bit} \quad \textbf{(3)}$$

The AES algorithm in SP-AES performs two functions namely, KeyGeneration and Rounding (as shown in figure 2). The KeyGeneration uses a Key Generator to evaluate the Keys used in AddKey. The objective of using this KeyGeneration function is that generating multiple keys from an initial key and using a unique key for each round, greatly increase the security of the system, ensuring packet transmission rate in a significant manner. The AES algorithm in SP-AES uses the key size of '$256\ bit$'. The first step performed by Key Generator is to accept a plain text as input and shift the word towards left once (i.e. ShiftLeftWord).

$$\boldsymbol{ShiftLeftWord \rightarrow ShiftLeft\ (P)} \quad \textbf{(4)}$$

From (4), the ShiftLeftWord operation '$ShiftLeftWord$' is performed using plain text 'P' as input. Followed by this a byte to byte substitution is performed where the output obtained from ShiftLeftWord function is fed as input to the 8-bit substitution box to perform multiplicative inversion.

$$\boldsymbol{ByteByteSub \rightarrow S\_(i,j)\ (ShiftLeftWord) \rightarrow \ 〖S'〗\_(i,j)\ (ShiftLeftWord)} \quad \textbf{(5)}$$

From (5), byte to byte substitution '$ByteByteSub$' is performed. Finally, a bit-wise XOR operation 'XOR' is performed where the resultant value is used as the key.

$$\boldsymbol{Key \rightarrow\ S_{i,j}\ XOR\ S'_{i,j}} \quad \textbf{(6)}$$

The value of key changes during each iterations and being a unique key security is ensured and therefore improves the packet transmission rate.

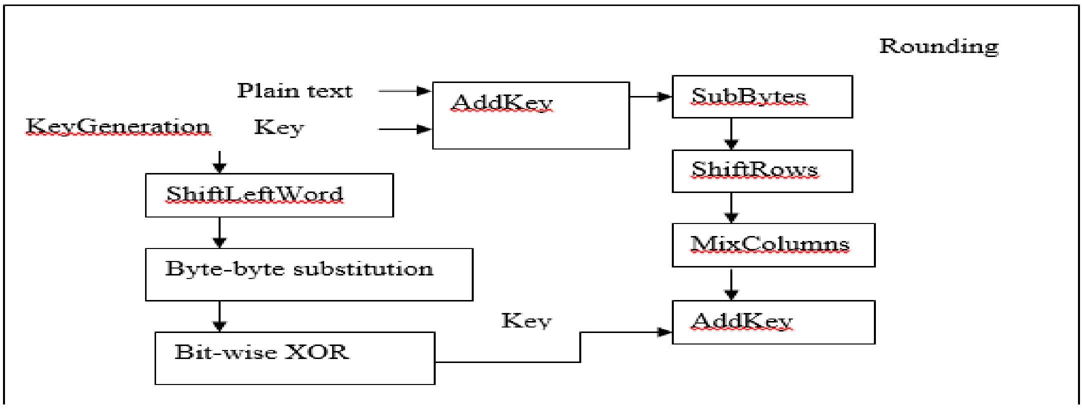

Figure 2 Block diagram of SP-AES model

On the other hand, the Rounding function starts its operation by substituting each byte in the state matrix (i.e. $S_{i,j}$) is replaced with the SubBytes in 8-bit 4 * 4 Substitution Box (as shown in figure 1 using eqn. 2). Followed by this, with the replaced SubBytes, ShiftRows function is performed where the first row remains unchanged and the second 'S_r', third 'T_r' and fourth 'F_r' row is shifted once to the left.

$$\boldsymbol{ShiftRows \rightarrow F_r ShiftLeft\ (S_r),\ ShiftLeft\ (T_r),\ ShiftLeft\ (F_r)} \quad \textbf{(7)}$$

The resultant values are then used as the input to perform MixColumns function. ThisMixColumns function takes four bytes as inputs and four bytes as outputs, where each input byte affects all four output bytes. Finally, the key obtained using KeyGeneration is then added to obtain the final key. This final key obtained is added to the mobile nodes whenever a data packet has to be sent the destination node. The packet structure using SP-AES is shown in figure 3.

Source Mobile Node SN_i	Key Key_i	Data Packets DP_i	Destination node 'DN'

Figure 3 SP-AES Packet structure

From figure 3, the SP-AES Packet structure includes, the source mobile node 'SN' ready for transmission, the key generated 'Key_i' using KeyGeneration and Rounding function, the destination node 'DN' to which the data packets 'DP_i' has to be sent. Figure 4 shows the SP-AES algorithm.

```
Input: Plain text 'P', Source Mobile Node $SN_i$, Key $Key_i$, Data Packets $DP_i$, Destination node 'DN'
Output: Improved packet transmission with reduced packet delay
Step 1: Begin
Step 2:    For each Source Mobile Node $SN_i$ with Data Packets $DP_i$
Step 3:       For each Plain text 'P'
Step 4:          Perform shift left using (4)
Step 5:          Perform byte-byte substitution using (5)
Step 6:          Perform XOR operation using (6)
Step 7:          Evaluate SubBytes operation using (2)
Step 8:          Evaluate ShiftRows operation using (7)
Step 9:          Evaluate MixColumns function
Step 10:      End for
Step 11:   End for
Step 12: End
```

Figure 4 SP-AES algorithm

As shown in the figure 4, the SP-AES algorithm is designed in such a way that multiple keys are generated using Key Generation function that in turn uses unique key during each iterations (i.e. for each source mobile node). This greatly increases the rate of security and therefore the packet transmission rate is improved reducing the packet delay in a significant manner.

2.2 Design of MD5-based malicious attack removal process

The MD5 algorithm operates on a 128-bit state, divided into four 32-bit words in mobile nodes (i.e. P, Q, R, S)to remove the malicious attack. MD5 are initialized to certain fixed constants, so that the cryptographic technique used to attempt on the stronger attacks in MANET.

The MD5 algorithm uses 512-bit data packets to be sent to modify the state. The processing of a data packet to be sent by the source mobile node to the destination node consists of rounds. Each round comprises of 16 similar operations based on the Cryptographic Function 'CF'. In addition to it a threshold value 'δ' is applied. The Cryptographic Function 'CF' applied for malicious attack removal is expressed as given below.

$$\boldsymbol{CF\ (Q, R, S) \rightarrow (Q\ AND\ R)\ OR\ (NOT\ Q\ AND\ S)} \qquad \textbf{(8)}$$

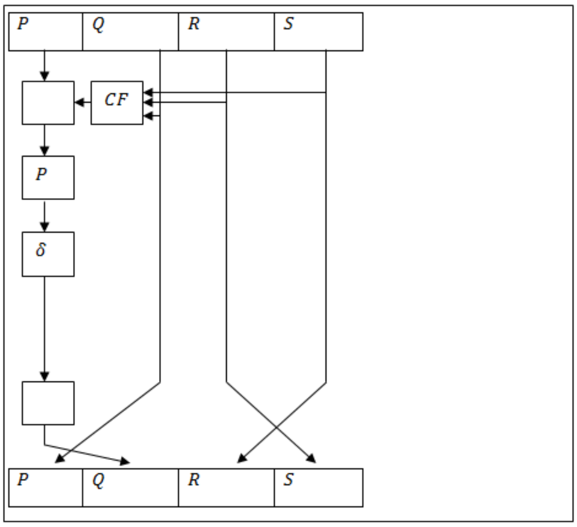

Figure 5 MD5-based malicious attack removal process

As shown in the figure 5, with the objective of removing the malicious attack, an MD5 algorithm that consists of 64 operations, grouped in four rounds of 16 operations is performed aiming at improving the true positive rate on detecting abnormal activities. The function used in MD5-based malicious attack removal process uses a non-linear function during each round.

The advantage of using the non-linear function in malicious attack removal is the provisioning of security and therefore improving the true positive rate on abnormal activities. As shown in the figure, a plain text 'P'' is given as input where 'δ' represents a threshold that differs during each iterations. Figure 6 shows the algorithmic description of MD5-based malicious attack removal (MD5-MAR).

```
Input: Plain text '$P$', Source Mobile Node $SN_i$, Data Packets $DP_i$, Destination node '$DN$', threshold value '$\delta$'
Output: Improved true positive rate on detecting abnormal activities
Step 1: Begin
Step 2:   For each Source Mobile Node $SN_i$ with Data Packets $DP_i$
Step 3:     For each Plain text '$P$'
Step 4:       Break the plain text '$P$' into chunks with 16 similar operations
Step 5:         Evaluate cryptographic function using (8)
Step 6:         Append threshold value '$\delta$' to the resultant cryptographic value
Step 7:     End for
Step 8:   End for
Step 9: End
```

Figure 6 MD5-based malicious attack removal algorithm

Finally, SP-AES and MD5-based malicious attack removal process fused together on the mobile nodes to communicate packets with high security. Therefore, the SP-AES algorithm and MD5-MAR algorithms offer data security and users authenticity using a mixture of two symmetric cryptographic techniques.

3. EXPERIMENTAL SETTINGS

Hybrid Symmetric Cryptography Technique (HSCT) in mobile ad hoc network uses the NS-2 simulator with the network range of 1400 * 1400 m size. For experimental purpose, the mobile nodes selected are 70 nodes and experiments are conducted with the aid of Destination Sequence Based Distance Vector DSDV as routing protocol for HSCT.

The moving speed of HSCT of each mobile node in MANET is about 20 m/s with a simulation rate of 30 seconds to perform data packet transmission between mobile nodes. The experimental settings used for conducing HSCT in mobile ad hoc networks are shown in table 1.

Experiment is conducted on the factors such as packet transmission rate, packet delay time, true positive rate on abnormal activities and security with respect to node density in MANET. The results of the metrics of HSCT are compared against the existing methods such Enhanced Adaptive ACKnowledgement (EAACK) [1] and Anonymous Location-Based Efficient Routing Protocol (ALERT) [2] in MANET respectively.

Table 1 Parametric settings

Parameters	Values
Simulator	NS 2.34
Simulation area	1400 m * 1400 m
Simulation time	30 sec
Mobile node density	10, 20, 30, 40, 50, 60, 70
Data packet	512 bytes/packet
Data packet transmission range	30 m, 60 m, 90 m
Movement model	Random waypoint

4. DISCUSSION

To validate the efficiency and theoretical advantages of the Hybrid Symmetric Cryptography Technique (HSCT) in mobile ad hoc network with Enhanced Adaptive ACKnowledgement (EAACK) [1] and Anonymous Location-Based Efficient Routing Protocol (ALERT) [2], simulation results under NS2 are presented. The parameters of the HSCT are chosen as provided in the experiment section.

4.1 Impact of packet transmission rate

The packet transmission rate is the percentage ratio of data packets received to the data packets sent at the destination end. The formulation of packet transmission rate is as given below.

$$PTR = \frac{DP_r}{DP_s} * 100 \qquad (9)$$

From (9), the packet transmission rate 'PTR' is measured using data packets sent 'DP_s' and data packets received 'DP_r'. Higher the packet transmission rate more efficient the method is said to be and measured in terms of Percentage (%).To better understand the effectiveness of the proposed HSCT, extensive experimental results are reported in table 2.

Table 2 Tabulation for packet transmission rate

Data Packet	Packet transmission rate (PPS)		
	HSCT	EAACK	ALERT
50	92	88	80
100	93	89	81
150	85	81	73
200	89	84	75
250	90	86	84
300	87	83	75
350	91	87	79

NS2 simulator is used to experiment packet transmission rate by analyzing the result using table and graph values. Results are presented for different number of data packets and the results reported here confirm that with the increase in the number of data packets, the packet transmission rate also gets increased, though not linear. This is because of the topology changes in MANET.

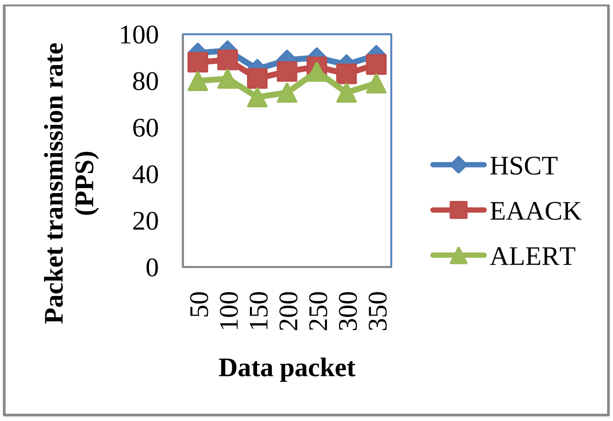

Figure 7 Measure of packet transmission rate

Figure 7 shows the packet transmission rate based on the data packet in mobile ad hoc network considered for experimental purpose. This proposed HSCT performs relatively well when compared to two other methods EAACK [1] and ALERT [2]. The packet transmission rate is improved in the HSCT by applying Substitution and Permutation-based Advanced Encryption Standard (SP-AES). By applying the Substitution and Permutation-based Advanced Encryption Standard (SP-AES), security for data packets are ensured through unique key for each round in MANET. Moreover, Advanced Encryption Standard performs KeyGeneration and Rounding in a significant manner. This helps in improving the packet transmission rate by 4.63% compared to EAACK [1]. With ShiftLeftWord and byte-to-byte substitution in HSCT, data packets are transmitted at the receiving end in a significant manner helps in improving the packet transmission rate by 12.77% compared to ALERT [2].

4.2 Impact of packet delay time

The packet delay time is the difference between the estimated time for the data packets to reach the destination node and the actual time to reach the destination node. The mathematical formulation of packet delay time is measured as given below.

$$PDT = \sum_{i=1}^{n} DP_i \left(Estimated_t - Actual_t\right) \qquad (10)$$

From (10), the packet delay time 'PDT' is measured based on the data packets 'DP_i' sent, the estimated time '$Estimated_t$' and the actual time '$Actual_t$' in MANET. Lower the packet delay time more efficient the method is said to be and is measured in terms of milliseconds.

Table 3 Tabulation for packet delay time

Data Packet	Packet delay time (ms)		
	HSCT	EAACK	ALERT
7	1.45	2.13	2.50
14	2.56	3.61	3.81
21	3.85	4.90	5.10
28	4.19	5.24	5.44
35	2.84	3.89	4.09
42	5.98	6.35	6.55
49	6.89	7.94	9.05

The targeting results of packet delay time using HSCT with two state-of-the-art methods [1], [2] in table 3 presented for comparison based on the data packets in mobile ad hoc network.

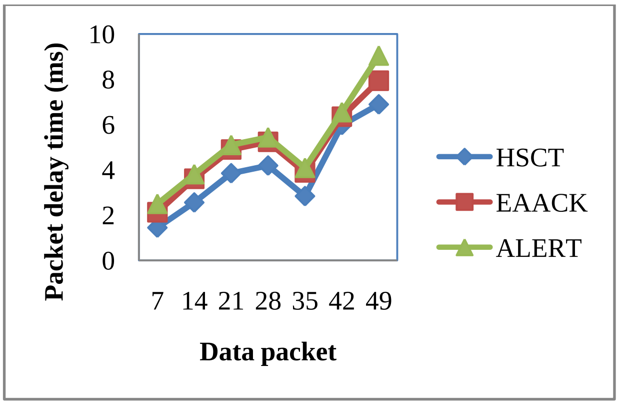

Figure 8 Measure of packet delay time

From figure 8, it is evident that the packet delay time is reduced using the proposed HSCT. The SP-AES algorithm with optimal strategy results in the reduced packet delay time in HSCT. With the application of SP-AES algorithm, Rounding function is produced at different time intervals resulting in the improvement of packet delay time (i.e. reducing the packet delay time). At the same time, in HSCT, the efficient shifting of second 'S_r', third 'T_r' and fourth 'F_r'

row is made in an efficient manner using ShiftRows function. With the shifting, the source mobile node performs data packet transmission and sends the data packet along with the key generated to the destination node in MANET. This in turn reduces the packet delay time using HSCT by 28.37% compared to EAACK [1] and 38.34% compared to ALERT [2] respectively.

4.3 Impact of True positive rate on Abnormal activities

True positive rate on abnormal activities is defined as the ratio of abnormal activities correctly identified as abnormal to the summation of abnormal activities correctly identified as normal and wrongly identified as abnormal. The mathematical formulation for true positive rate on abnormal activities is given as below.

$$TPR_{detecting\ \ abnormal\ \ activities} = \frac{Abnormal_{\ correctly\ \ identified}}{Abnormal_{\ correctly\ \ identified} + Abnormal_{\ wrongly\ \ identified}} * 100 \quad (11)$$

The true positive rate is measured in terms of percentage (%). Higher the true positive rate more efficient the method is said to be.

Table 4 Tabulation for true positive rate on abnormal activities

Node density	True positive rate on abnormal activities (%)		
	HSCT	**EAACK**	**ALERT**
10	84	67	61
20	89	63	55
30	85	68	60
40	88	71	63
50	82	65	57
60	84	67	59
70	87	70	62

As listed in table 4, HSCT measures the true positive rate on abnormal activities during data packet transmission in MANET with respect to node density. It is measured in terms of percentage (%). The true positive rate on abnormal activities in MANET using HSCT offers comparable values than the state-of-the-art methods.

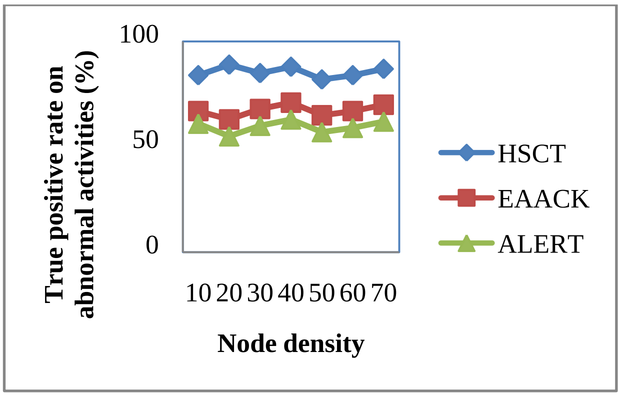

Figure 9 Measure of true positive rate on abnormal activities

Figure 9 presents the variation of true positive rate on abnormal activities with respect to node density in MANET. All the results provided in figure 9 confirm that the proposed HSCT significantly outperforms the other two methods, EAACK [1] and ALERT [2]. The true positive rate on abnormal activities is improved in the HSCT using the MD5-based malicious attack removal process. With the application of MD5-based malicious attack removal process, cryptographic technique to combat against stronger attacks in MANET is ensured. Followed by this, Cryptographic Function is applied to the source mobile nodes ready for data packet transmission. This in turn improves the true positive rate on abnormal activities by 21.32% compared to EAACK. As a result true positive rate is improved in HSCT using MD5. Moreover, 64 operations using MD5 are grouped in four rounds of 16 operations improves the true positive rate by 30.34% compared to ALERT.

4.4 Impact of Security

Security is obtained based on the difference between the data packets being transmitted and the data packets dropped during transmission. The mathematical formulation for security is as given below.

$$\boldsymbol{S = (DP_t - DP_d)} \qquad \textbf{(12)}$$

From (12), security 'S' is measured using data packets transmitted 'DP_t' and data packets dropped 'DP_d' respectively. Security is measured using packets per second (PPS). Higher the security, more efficient the method is said to be.

Table 5 Tabulation for security

Data Packet	Security (PPS)		
	HSCT	**EAACK**	**ALERT**
50	47	44	42
100	85	77	69
150	135	128	120
200	189	175	170
250	235	215	208
300	279	265	251
350	339	328	320

In table 5 we show the analysis of security for data packets being transmitted and protecting the data packets from malicious attacks with respect to number of data packets in the range of 50 to 350. It is measured in terms of Packets Per Second (PPS).

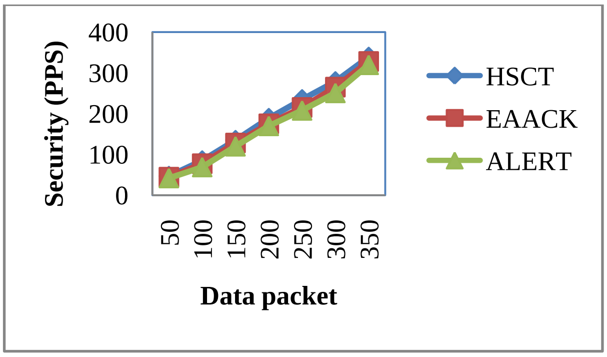

Figure 10 Measure of security

Figure 10 shows the security using three methods HSCT, EAACK and ALERT. From the figure it is evident that the security is improved using HSCT. This confirms the efficiency of the proposed technique HSCT. The security in HSCT is improved by applying MD5-based malicious attack removal (MD5-MAR) algorithm. Furthermore by applying SP-AES and MD5-based malicious attack removal process fused together on the mobile nodes to communicate data packets higher security rate is ensured. With the application of mixture of two symmetric cryptographic techniques, SP-AES and MD5-MAR, security with unique key and cryptographic function is provided in HSCT. This in turn improves the security by 6.45% compared to EAACK and 11.10% compared to ALERT.

5. CONCLUSION

In this paper, Hybrid Symmetric Cryptography Technique (HSCT) is provided based on the novel mixture of two symmetric cryptographic techniques using SP-AES algorithm and MD5-MAR for MANET. This technique reduced packet delay time and improves the true positive rate on abnormal activities in Mobile Ad Hoc Network. As the technique uses the SP-AES algorithm in a dynamic manner, it improves the packet transmission rate in MANET through efficient selection of unique key for each round whenever a source mobile node has to transmit packets. As a result, the proposed SP-AES algorithm performs data packet transmission in an efficient manner reducing the packet delay time in an efficient manner and helps in improving the security. By applying the MD5-based malicious attack removal process in HSCT, true positive rate on abnormal activities is improved and overcomes the vulnerability of computation overhead in MANET. Finally, with the application of two algorithms, SP-AES and MD5-MAR, high security to information on MANET is ensured. Different mobile nodes with varied data packet sizes on MAENT using HSCT carefully analyze the data packet transmission and therefore significantly secure the mobile network system from malicious attacks in MANET. A series of simulation results are performed to test the packet transmission rate, packet delay time, true positive rate on abnormal activities and security is presented. Experiments conducted on varied simulation runs shows improvement over the state-of-the-art methods. The results show that HSCT offers better performance with an improvement of packet transmission rate by 8.70% and enhances the security by 8.77% compared to EAACK and ALERT respectively.

6. REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, “EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE Transactions on Industrial Electronics, Volume 60, Issue 3, March 2013, Pages 1089-1098.

[2] Haiying Shen, and Lianyu Zhao, “ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs”, IEEE Transactions on Mobile Computing, Volume 12, Issue 6, June 2013, Pages 1079-1093.

[3] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, and Helen Tang, “Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks”, IEEE Transactions on Wireless Communications, Volume 10, Issue 9, September 2011, Pages 3064-3073.

[4] Ming-Yang Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems”, Elsevier, Computer Communications, Volume 34, Issue 1, 15 January 2011, Pages 107–117.

[5] Thomas F. La Porta, Gaia Maselli, and Chiara Petrioli, “Anticollision Protocols for Single-Reader RFID Systems: Temporal Analysis and Optimization”, IEEE Transactions on Mobile Computing, Volume 10, Issue 2, February 2011, Pages 267-279.

[6] Kiran Mehta, Donggang Liu, “Protecting Location Privacy in Sensor Networks against a Global Eavesdropper”, IEEE Transactions on Mobile Computing, Volume 11, Issue 2, February 2012, Pages 320-336.

[7] Hyun-A Park, Jong Wook Hong, Jae Hyun Park,Justin Zhan, and Dong Hoon Lee, “Combined Authentication-Based Multilevel Access Control in Mobile Application for DailyLifeService”, IEEE Transactions on Mobile Computing, Volume 9, Issue 6, June 2010, Pages 824-837.

[8] Shengbo Yang, Chai Kiat Yeo, and Bu Sung Lee, “Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks”, IEEE Transactions on Mobile Computing, Volume 11, Issue 1, January 2012, Pages 111-124.

[9] Anh Le, and Athina Markopoulou, “Cooperative Defense Against Pollution Attacks in Network Coding Using SpaceMac”, IEEE Journal on Selected Areas In Communications, Volume 30, Issue 2, February 2012, Pages 442-449.

[10] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran, “Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks”, IEEE Transactions on Mobile Computing, Volume 9, Issue 8, August 2010, Pages 1119-1133.

[11] Haitao Wu, Zhenqian Feng, Chuanxiong Guo, and Yongguang Zhang, “ICTCP: Incast Congestion Control for TCP in Data-Center Networks”, IEEE/ACM Transactions on Networking, Volume 21, Issue 2, April 2013, Pages 345-358.

[12] Zhichao Zhu, and Guohong Cao, “Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System”, IEEE Transactions on Mobile Computing, Volume 12, Issue 1, January 2013, Pages 51-64.

[13] Eugene Y. Vasserman and Nicholas Hopper, “Vampire attacks:Draining life from wireless ad-hoc sensor networks”, IEEE Transactions on Mobile Computing, Volume 12 Issue 2 , Year 2013, Pages 1-15.

[14] Arif Selcuk Uluagac, Raheem A. Beyah, Yingshu Li, and John A. Copeland, “VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks” IEEE Transactions on Mobile Computing, Volume 9, Issue 7, July 2010, Pages 994-1006.

[15] Shafiullah Khan, Kok-Keong Loo, and Zia Ud Din, “Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks” International Arab Journal of Information Technology, Volume 7, Issue 4, October 2010, Pages 435-440.

[16] M. Rajesh Babu, S. Moses Dian, Siva Chelladurai, and Mathiyalagan Palaniappan, "Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version", Hindawi Publishing Corporation, Scientific World Journal, Volume 2015, August 2015, Pages 1-11.

[17] Jaeun Choi, Gisung Kim, and Sehun Kim,"A Congestion-Aware IDS Node Selection Method for Wireless Sensor Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2012, June 2012, Pages 1-7.

[18] Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, April 2013, Pages 1-7.

[19] A. L. Sandoval Orozco, J. GarciıaMatesanz, L. J. Garcia Villalba, J. D. Marquez Diaz, and T-H Kim, "Security Issues inMobile Ad Hoc Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2012, October 2012, Pages 1-6.

[20] Mouhannad Alattar, Francoise Sailhan, and Julien Bourgeois, "On Lightweight Intrusion Detection: Modeling and Detecting Intrusions Dedicated to OLSR Protocol", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, April 2013, Pages 1-21.