TEST Engineering & Management

November /December 2020
ISSN: 0193-4120 Page No. 387-406

Hybrid Key Cryptography based Intrusion Detection System in Manet

Prolay Ghosh[1], Dr. Nisarg Gandhewar[2]

[1] Research Scholar, Department of Computer Science and Engineering, Dr. A.P.J Abdul Kalam University, Indore, M.P.

[2] Research Guide, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, M.P.

Article Info
Volume 83
Page Number: 387- 406
Publication Issue:
November /December 2020

Article History
Article Received :*25 October 2020*
Revised: *22 November 2020*
Accepted: *10 December 2020*
Publication: *31 December 2020*

Abstract

A mobile network for ad hoc (MANET) is a mobile device network that is free of wires and which is continuously established. Each MANET device may move in any direction independently, changing its connections frequently to another device. Each MANET node should be a router that does not relate to traffic to its own end. The main challenge to build a MANET is the continuous maintenance of information required on each device for proper traffic. These networks may operate on their own or be connected to the Internet. One or more transceivers may be included between nodes. Between nodes. Between nodes. This leads to an autonomous topology that is highly dynamic. Restricted wireless communication and high-level mobility nodes need collaborative nodes to provide the required connectivity, constantly changing the underlying network to ensure the demand is continuously fulfilled.

Keywords: Hybrid, Cryptography, Intrusion, Detection, Manet

INTRODUCTION:

Wireless networking is the medium of choice for many applications at present. Modern production techniques also allow smaller, more mobile devices to have more sophisticated capabilities. One of the major advantages of wireless networks is the ability to allow communication among different parties and maintain mobility. Nevertheless, this communication is limited to the number of transmitters. This means

November /December 2020
ISSN: 0193-4120 Page No. 387-406

two nodes cannot interact if the distance between the two nodes exceeds the communication range of their own. Mobile ad hoc networks (MANETs) address this problem and allow the data transmission between the intermediate parties.

In a range of wireless communications, Mobile MANET's combination of wireless and high-node mobility means that nodes must cooperate to develop essential networks and transform the underlying network dynamically, ensuring their demands are continuously met. The MANET dividing into two networks, one store and one store. This is achieved via In one hop network, all nodes in the same range communicate directly with each other. Nodes instead use intermediate nodes when the destination node is outside their radio range when it is transmitted over a multi-hop network. MANETs were proposed in many areas, including rescues, tactical operations, environmental monitoring, conferences [1].

Intrusion detection is an essential element of defense against attackers or hackers of the cyber infrastructure. Techniques such as the filtering of router rules or firewalls for protection of intrusion fail to thwart such assaults.

Thus, intruders still exist and they should thus be recognized no matter how effectively a system is secured. Intrusion detection systems are becoming an important component of computer system and security. An intrusion detection system detects various kinds of hostile nodes that may undermine computer system security and confidence. If MANET understands how to identify attackers when they join the network, we can first eliminate the potential harm produced by affected nodes.

IDSs complement current proactive methods and are typically the second level of MANETs. Intelligent monitoring mechanisms are needed by IDS to effectively monitor and identify attempts at security violation throughout the anticipated lifespan of the network. As a concept, hybrid cryptography has two different terms: 'Hybrid' and 'Cryptography.' The encrypting and decryption is done by itself on two pillars. It has two major kinds: symmetrical encryption and asymmetric encryption. It consists of two types [2].

The term "Hybrid" means a combination of two mostly recognized forms of cryptography, i.e. the dominance of both characteristics into one system to enhance the power of the encryption process. Therefore, hybrid cryptography= symmetric key encryption + asymmetrical key encryption Therefore we must separately comprehensive the characteristics of each of them in terms of hybrid cryptography in order to justify this merging and the feasibility of using such system for protection against safety violations.

A hybrid encryption system is a mixture focusing mostly on merging asymmetric encryption with symmetric encryption efficiency. With data transmission, hybrid coding with symmetric coding may be done through single session keys. Symmetric key-

cryptography uses a system called a scheme for data encapsulation. It is focused on how securely our information may be made confidential by concealing it with the single sharable key known as the secret key or the private keypad between its sender and recipient [3].

Since just a sharable key, the symmetrical technique needs a symmetrical name. The method may be shown using the following notes: send 'S' to the recipient, 'M' to the recipient, 'R' Hence, the sender's encryption, 'E,' i.e. E linke, M linke, K linse.

This phase may be seen as the locking of the data with K. Now, when the encrypted data is received at the end of the recipient, it must be decrypted, in order to access the data by using the same key, "K." Thus, decrypting, 'D' carried out at the conclusion of a receiver i.e. message, M to encrypted information, E to key, K The following method can be anticipated as highly efficient for the short-length message(s), however it may be impossible to retain this scale of efficiency when applying for long messages [4].

It is because of the single key that may be readily split between the two parties. Therefore, the concept came into being to encrypt the encrypted data, i.e. double encryption.

PROPOSED INTRUSION DETECTION SYSTEM USING HYBRID KEY CRYPTOGRAPHY (IDS-HKC) METHOD

Encryption rule is a public key (sendered), while the private key is the decryption rule (known only by the receiver). Encryption encodes the message to be sent so that the other nodes cannot comprehend the encrypted message (cipher text). Public key encryption is used to solve security and sender identification problems.

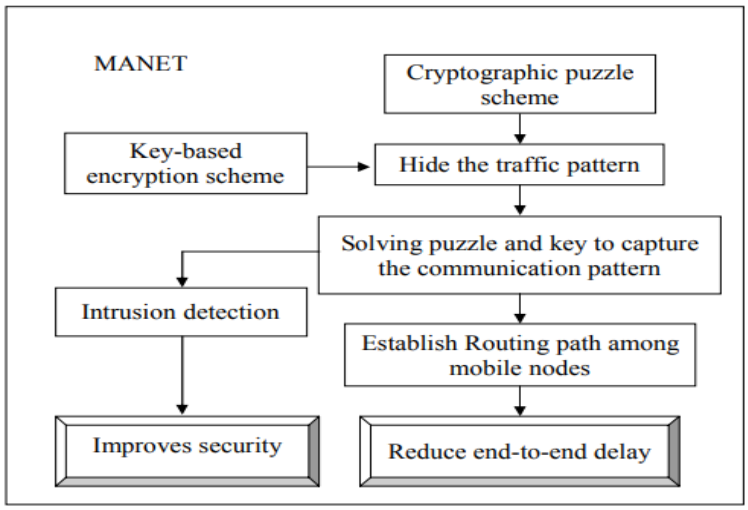

Figure 1 Architecture of proposed IDS-HKC method

Cryptographic Puzzle Scheme

The ongoing availability of the wireless media to link partial nodes depends on wireless networks. Due of the openness of this medium, it is vulnerable to numerous security risks. All of us with a transceiver will cave into wireless communications, inject fake signals or real jam messages. Criptural methods may prevent falls and injection of messages, but jamming is much more difficult to deal with. There's no jamming. The attack on cellular networks was demonstrated to be improved to include an extreme denial of service (DoS). By delivering a persistent jam signal or many short jamming pulses the opponents interfere in the simplest manner when message is received [5].

Our puzzle concealing technique is cryptographeric. The main reason for these puzzles is to force a puzzle recipient to conduct a predefined sequence of calculations and confidentiality. It relies on the difficulty of the solver and calculation abilities to get the problem answer. The advantage of the puzzle system is that the PHY layer settings are unaffected for its safety. In this research, wireless networks addressed the problem of targeted jamming assaults and considered it an adversary paradigm under which the Jammer belongs to a network that was being attacked. The jammer classifies the first few symbols of continued transmission via real-time decoding of ted packets [6].

The role-based access architecture for cryptographic puzzles contributes to many security applications. Merklle utilizes the cryptographic puzzle system for the IDS-HKC method (Merklle, 1974). The MANET node pattern is hidden by puzzles. The traffic pattern includes information about the source, destination and connections. Pattern of traffic. If a mobile node in MANET wants to move, the puzzle generated by the sender must be resolved using any computation. Authorized users only know the resolution form of puzzles and thus intruders while trying to capture the traffic pattern. The cryptographic puzzle function is employed. If you consider 'Alice' or 'Bob' contact, for example. The Eavesdroppers in MANET attempts to access records of "Alice" or "Bob." Figure demonstrates stable Bob and Alice correspondence [7].

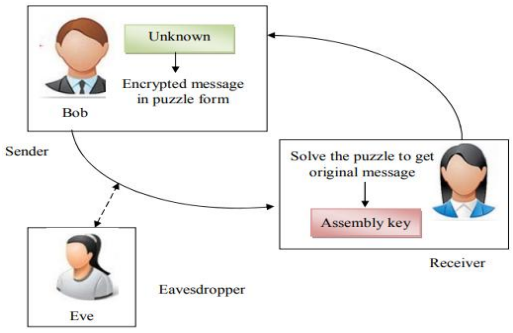

Figure 2 Secure communication among Bob and Alice

November /December 2020
ISSN: 0193-4120 Page No. 387-406

The next steps will be shown in Figure if 'Bob' attempts to pass 'Alice' to a message. All parties agree on a shared secret by exchanging messages. First "Bob" presents a wide variety of puzzles with minor problems in computer determination (i.e. feasible for "Alice" to solve the puzzle). The romance is in the form of an unknown encrypted message (which is short enough to permit a brute force attack). 'Bob' sends the problems to 'Alice.' Now 'Alice' blindly chooses one of the problems and resolves it. 'Alice' has an encoded response that contains both a key and an identification when the problem is solved. This mounting key enables the interactions between 'Alice' and 'Bob.' Finally, the key to safe communications is "Alice" and "Bob"

The mystery 'Alice' is not answered in 'Eve' and 'Bob.' 'Eve' costs more to the computer than 'Alice,' where 'Bob' resolve both issues. The cost of 'Eve' is more expensive. Thus, contact with the IDS-HKC system proposed in MANET is not disturbed by the intruders.

Input: Mobile nodes '$\{MN_1, MN_2 \ldots MN_n\}$', sender '$S$', receiver '$R$', packet '$m$', random key '$k$' and timestamp '$tp$'
Output: Generate puzzle cryptography for security
Step 1: Begin
Step 2: If 'S' wants to send a packet 'm' to 'R'
Step 3: 'S' selects random key '$k\{0,1\}$' to generate puzzles
Step 4: $P = puzzle\ (k, tp)$
Step 5: 'S' broadcast 'P' to network along with cipher text
Step 6: $C = Ek\ (\pi, (m))$
Step 7: At receiver, 'R' received cipher text C' and puzzle P'
Step 8: First 'R' solves the puzzle $K' = solve(P)$
Step 9: Then 'R' converts cipher text into Plain text
Step 10: End

Figure 3 Puzzle cryptography Algorithm

Often cryptographic riddles were used to remove denial-of-service attacks from the network. The puzzle encryption methods for the proposed IDS-HKC process are shown in Figure. The cryptographic puzzle algorithm generates puzzles at the transmitter so that the recipient's hand is secured. The sender selects first the random key to create the "tof,1" cryptographic puzzles. The node then transmits the message to the network as a puzzle-like cipher text. The material is ultimately converted into simple words by resolving the problem of the recipient

Key-based Encryption Scheme

In order to hide the pattern of the traffic packet format, the main encryption techniques are also utilized in the IDS-HKC approach. The next stage is to resolve the key-based encryption in the MANET that is some kind of role-based access restriction after the puzzles are solved. The user must know the solution technique of certain key systems in order to retrieve the original frame format of a communication pattern. The suggested IDS-HKC technique is shown in Figure. Encryption is accomplished by using conventional encryption software and hardware for data protection, such as pictures and videos. In the case of all files that includes characters, numbers and symbols, a new symmetrical key cryptography technique is used in the IDS-HKC method for encryption and decryption [8]

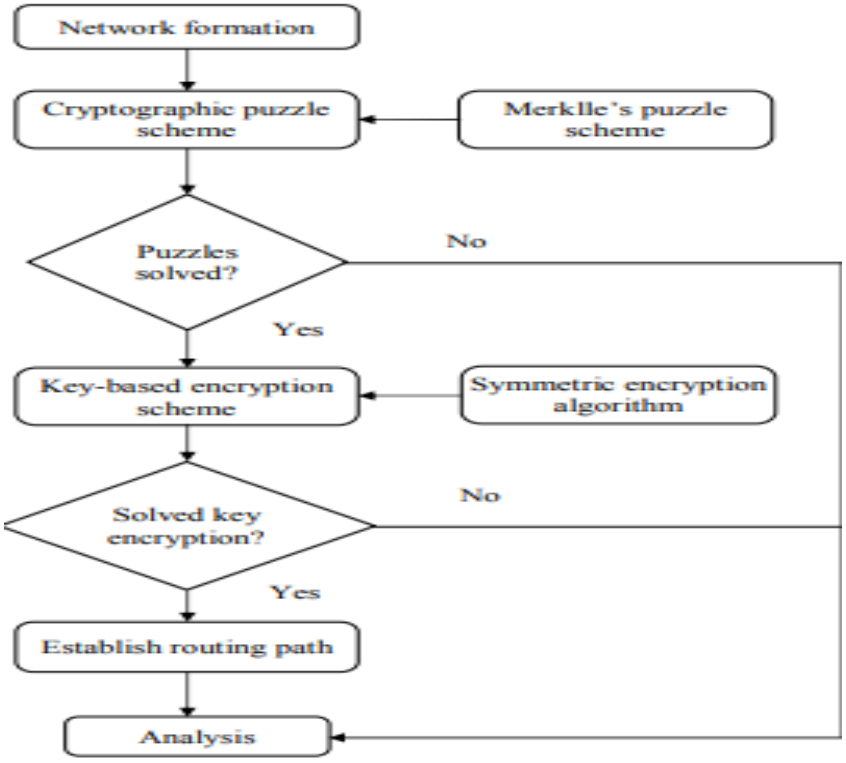

Figure 4. Flow process of proposed IDS-HKC method for security enhancements in MANET

After resolution of the cryptographic problem, MANET mobile Nodes use key-based encryption methods to increase security further. For the key-based encryption, a symmetric encryption method is used. Also solves the key if the mobile node. The route path to future communication in MANET is chosen based on the encryption. The node is otherwise an invader that is readily identified using the IDS-HKC technique.

November /December 2020
ISSN: 0193-4120 Page No. 387-406

Establish Routing Path

In MANET, the malevolent neighbor transporting packets to the destination is experiencing numerous difficulties in security. For the valid mobile nodes, thus, puzzle solving and key solving are used. The mobile node in MANET allows the communication pattern to be accessed and offers the routing route after successfully solving puzzles and resolving key. This routing route is defined in the network based on the packet information including the destination node specifics. For all MANET nodes the routing table is utilized to get information about the routes you found.

All other nodes in the network utilize routing table information about a mobile node and update it periodically. Multipath routing algorithms are intended to divide traffic loads and transfer them concurrently to one destination via two or more distinct routes. In this work, we present a novel routing system for balancing the load of the network while maintaining efficient network performance.

Mobile Adhoc network includes autonomous nodes that may dynamically learn their topology and utilize packet router information between nodes. The packets are transported from source to destination via several hops between nodes. As nodes in MANET are movable, the routing route often varies causing packet losses. As a consequence, MANETs are low for packet delivery. MANET has emerged for catastrophe management and emergency communication as the most promising application. The telecommunications infrastructure is failing in the event of floods or earthquakes and the MANET solution to the issue is evident in the rescue sector [9].

The dependability of MANET with respect to the increased packet delivery ratio must therefore be guaranteed. Improving routing endurance with the node location prediction is promising to enhance routing confidence in MANETs. Many prediction techniques for node locations were suggested. Literature suggested node localization prediction based on previous node positions, trajectory based location estimates, network structure etc. In the literature prediction methods for node placement were suggested in the categories Deterministic, Stochastic, and History-based and Heuristic

This is the architecture of the IDS-HKC approach. The IDS-HKC procedure secures the routing route between the mobile nodes. The combination of the encryption system and key-base encryption system to hide the invader traffic pattern is the means to accomplish this. This safety is obtained. The intrusion detection is therefore done efficiently and the latency from one end to another is further reduced to the target node.

EXPERIMENTAL EVALUATION

The proposed IDS-HKC method is implemented by using NS2 simulator. Let us consider 500 mobile nodes which are deployed in the square area of 1500 m * 1500 m for experimental purpose

Table 1 Simulation settings

Parameter	Value
Simulation area	1500 m * 1500 m
Number of mobile nodes	50 to 500
Number of data packets	10 to 100
Size of data packets	50 to 500 KB
Simulation time	70 ms
Traffic model	Constant Bit Rate (CBR)
Mobility model	Random Way Point
Routing protocol	DSR
Node speed	0 – 20 m/s
Pause time	500 s

The model Random Way Point is used to provide nodes with mobility. A range 10 to 100 is used for the number of data packets. For doing simulations, the DSR protocol is utilized. The parameters for the proposed IDS HKC technique are shown in Table 3.1. Table 3.1. IDS-HKC performance is determined by factors including throughput, overhead routing, packet loss rate, intrusion detection rate and latency from end to end.

RESULT ANALYSIS AND DISCUSSION

The proposed intrusion detection system used by Tarek Sheltami (Tarek Sheltami, 2014) and Certificates-on-demand Public Key Management (CLPKM) protocol developed by Soumyadev Maity & Hansdah, using the IDS-HKC method, is compared with the existing methodologies, namely Adaptive Three Acknowledgements, A3ACKs. Tables and graphs are used to compare the suggested IDS-HKC technique with the current state of the art [10].

The overhead routing is measured as the extra amount of total routing packets for end-to-end network communication. The overhead routing is stated as follows mathematically.

$$RO = \frac{Number\ of\ packets\ additionally\ added}{total\ number\ of\ packets} * 100$$

From equation routing overhead 'RO' is calculated in terms of percentage (%). In case of low routing overhead, more efficiency is achieved.

Table 2 Measurement of routing overhead

Number of data packets	Routing overhead (%)		
	Existing A3ACKs	Existing CLPKM	Proposed IDS-HKC
10	22	25	17
20	26	29	21
30	29	33	24
40	32	37	29
50	36	40	32
60	38	44	35
70	42	46	39
80	46	50	42
90	49	52	44
100	52	55	47

Table 3.2 shows the overhead routing for transmitting data packets between the MANET mobile nodes using the IDSHKC and current techniques suggested. For experiment purposes, the numbers of data packets are extracted as input and ranged from 10 to 100. Table 3.2 shows that overhead routing is also improved by increasing the amount of data packets for all processes. In contrast to the current A3ACK and CLPKM techniques, the suggested IDS-HKC method offers minimal overhead routing. Figure 3.5 displays the overhead routing for the IDS-HKC process and comparisons with the current techniques A3ACKs and CLPKM are conducted. In comparison to current techniques the IDS-HKC method efficiently minimizes overhead routing.

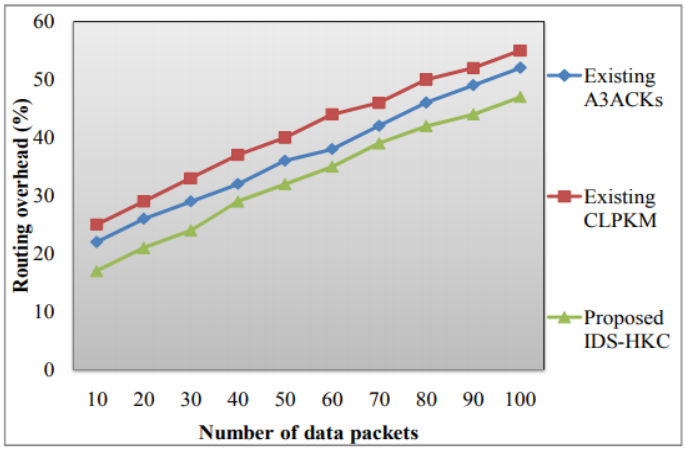

Figure 5. Estimation of routing overhead

November /December 2020
ISSN: 0193-4120 Page No. 387-406

By integrating the cryptographic puzzle and the key-based encryption system for the purposes of hiding the invader nodes, this decrease of overhead routing in the IDS-HCC technique is accomplished. Thus, intrusion detection based on their behavior is successfully conducted. As a result, routing overhead is decreased by 14 and 27% in comparison with the current A3ACK and CLPKM techniques in the MANET system utilizing the IDS-HKC approach [11]..

Performance of Throughput Rate

The 'TR' rate is called as a ratio of the number of packets successfully acquired at the Mobile Node Destination to the number of packets sent from the source node in the proposed IDS-HKC technique. Thus, the rate of transmission is calculated as follows mathematically.

$$TR = \frac{number\ of\ packets\ successfully\ received}{total\ number\ of\ packets\ sent} * 100$$

From above equation, 'TR' is computed with percentage (%). In case of high throughput rate, more efficiency is achieved.

Table 3 Comparison of throughput rate

Number of data packets	Throughput rate (%)		
	Existing A3ACKs	Existing CLPKM	Proposed IDS-HKC
10	69	63	74
20	71	64	75
30	72	67	77
40	73	68	78
50	75	69	80
60	76	71	81
70	78	72	82
80	79	74	84
90	80	75	85
100	82	77	88

Table 3 shows the throughput rate with respect to the number of data packets in MANET using the proposed and existing methods. Number of packets is extracted as input which is varied between the range of 10 and 100 for the purpose of conducting test. Table shows that, the throughput rate is increased with the respective increase in number of data packets for all the methods. However, the proposed IDS-HKC method significantly enhances the throughput rate when compared to the existing A3ACKs and CLPKM methods [12].

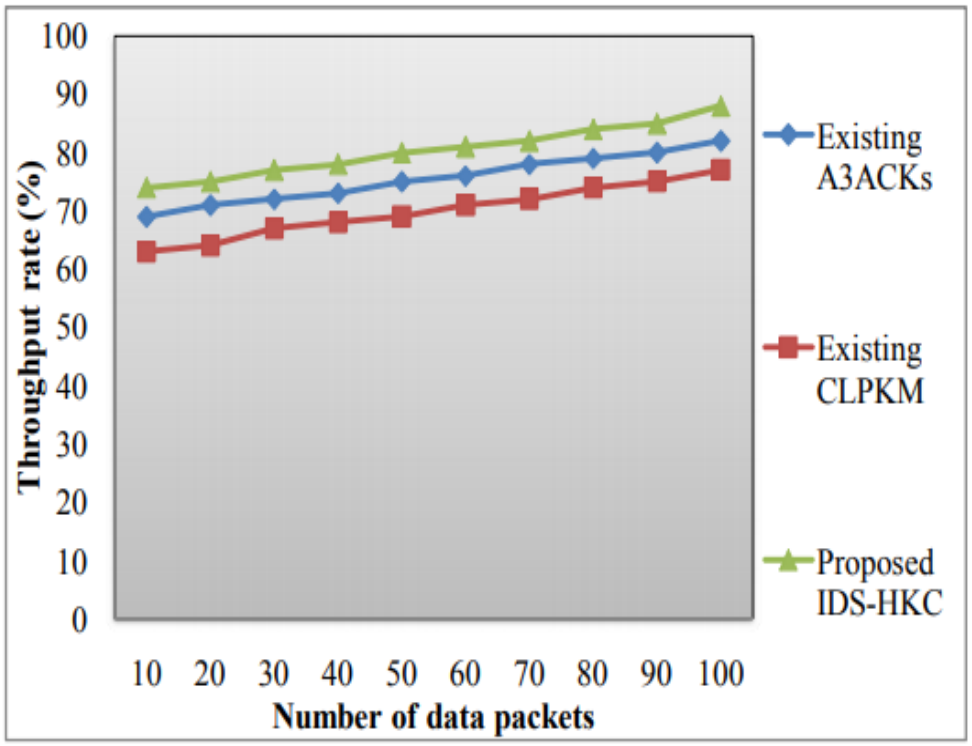

Figure 6 Assessment of throughput rate

Figure 6 shows the IDS-HKC throughput rate value and the techniques A3ACK and CLPKM are compared with the current approach. In comparison to current techniques, the IDS-HKC method significantly increases performance. The IDS-HKC technique uses the symmetric encryption algorithm for key-based encryption to accomplish this efficient increase in the flow rate. The mobile node is chosen for the route path for further communication inside the MANET to solve puzzles and key-based encryption. Thus in relation to the current A3ACK and CLPKM techniques, the throughput rate of the IDS-HKC method is increased by 6% and 13% [14].

Function of End-to-End Delay

End-to-end delay in MANET is defined as the amount of time taken to perform routing and data transmission. End-to-end delay is mathematically formulated as follows.

$$ED = Routing_d + Transmission_d$$

From equation, end-to-end delay 'ED 'is measured in terms of milliseconds (ms). In case of low end-to-end delay, the method is assumed to be more efficient.

Table 4 Comparison of end-to-end delay

Size of data packets (KB)	End-to-end delay (ms)		
	Existing A3ACKs	Existing CLPKM	Proposed IDS-HKC
50	14.5	16.4	12.4
100	15.9	17.6	13.6
150	16.2	18.7	14.8
200	17.6	20.3	16.1
250	18.9	21.4	17.5
300	20.8	22.8	18.2
350	21.7	23.9	20.3
400	23.6	25.1	21.8
450	24.1	26.7	22.4
500	26.3	27.9	23.9

Table shows the amount of database packets inside MANET for the IDS-HKC suggested and current techniques to be delayed from end-to-end. Data packets are retrieved for experimental purposes in the range of 50 and 500. In Table 3.4, the end-to-end latency for all techniques is likewise enhanced to increase data package sizes. In comparison with current techniques, the suggested IDS-HKC method lowers substantially the end-to-end latency.

Figure illustrates the IDS-HKC method's end-to-end lateness and compares it to current techniques A3ACKs and CLPKM, in particular. In comparison with the current techniques, the IDS-HKC method effectively decreases end-to-end latency. The IDS-HKC technique uses both encryption puzzles and key-based crypting methods in MANET to efficiently reducing the end-to-end latency.

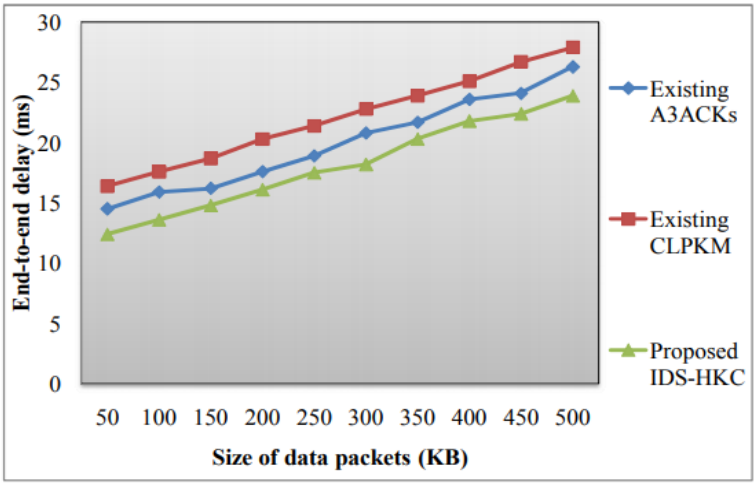

Figure 7 Computation of end-to-end Delay

By using these safety systems, authorized nodes simply transmit messages quicker to their destination. As a result, MANET's end-to-end latency utilizing the suggested IDS-HKC technique has been decreased by 11% and 23% in comparison with current A3ACKs and CLPKM methods.

Impact of Packet Loss Rate

The rate of loss of paquets is determined by the proportion of paquets dropped by the neighboring mobile nodes and transmitted by source mobile nodes to the total data paquets. The packet loss rate mathematical formulation is shown as follows.

$$PLR = \frac{Number\ of packets dropped}{total\ number\ of\ packets\ sent} * 100$$

From equation, packet loss rate PLR is measured in terms of percentage (%). If the packet loss rate is low, the method is said to be more effective.

Table 5 Measurement of packet loss rate

Number of data packets	Packet loss rate (%)		
	Existing A3ACKs	Existing CLPKM	Proposed IDS-HKC
10	27	31	23
20	29	33	25
30	32	36	28
40	35	38	32
50	37	41	34
60	40	45	37
70	42	47	39
80	45	48	42
90	47	50	44
100	48	53	45

During data packet transmission, Table 3.5 illustrates the packet loss rate for MANET utilizing the proposed IDS-HKC as well as the current processes. For experiment purposes, the number of data packets should be considered input and varies from 10 to 100. It is evident in Table 3.5 that the loss rate of packets is also improved for all techniques and the quantity of data packets increases. However, in comparison with current A3ACKs and CLPKM techniques, the suggested IDS-HKC method presents a minimal packet loss rate

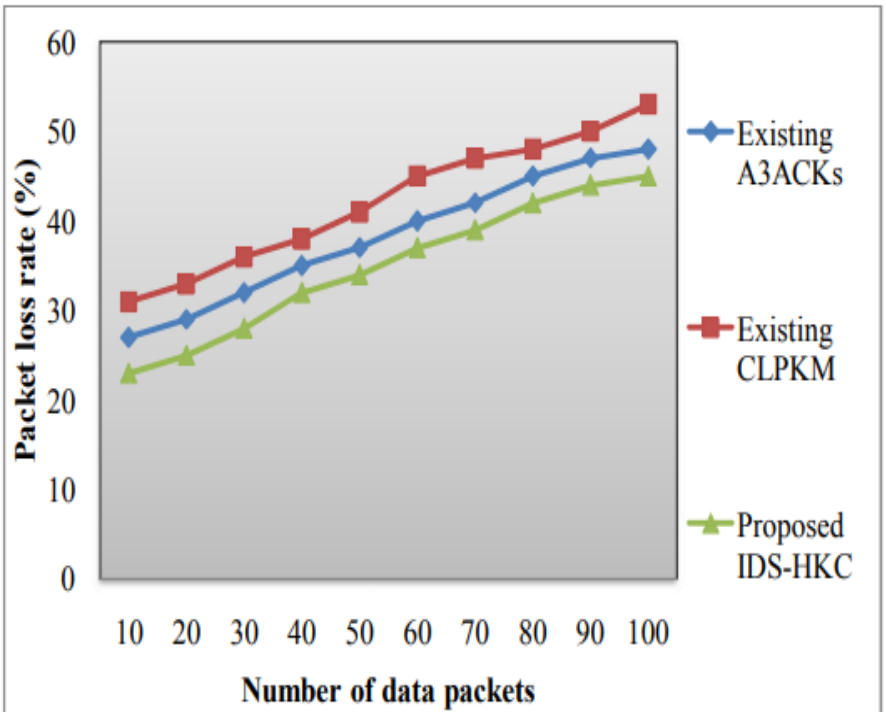

Figure 8 Assessment of packet loss rate

Figure shows a rate of packet loss for the IDS-HKC technique and the methods A3ACK and CLPKM are comparable to current approaches. In comparison with the current techniques, the IDS-HKC method effectively decreases end-to-end latency. The IDS-HKC technique combines cryptographer puzzle and key-based encryption methods in MANET for this efficient decrease in packet losses. It identifies the genuine nodes that do not drop the received packets. Consequently, packet loss rate in MANET is decreased by 10 and 22 percent in comparison to the corresponding A3ACK and CLPKM techniques utilizing the suggested IDS-HKC approach.

Performance of Intrusion Detection Rate

IDR is computed by the ratio of detected intruder nodes to the total number of available intruder ones. It is demonstrated using the following equation

$$IDR = \frac{numberofdetectedintrudernodes}{totalnumberofintrudernodes} * 100$$

From equation, intrusion detection rate 'IDR' is computed with percentage (%). In case of high intrusion detection rate, more efficiency is achieved.

Table 6 Comparison of rate of intrusion detection

Mobile nodes	Rate of intrusion detection (%)		
	Existing A3ACKs	Existing CLPKM	Proposed IDS-HKC
50	65	60	71
100	66	61	72
150	68	63	74
200	70	64	76
250	72	66	77
300	73	68	79
350	74	69	81
400	77	71	82
450	78	72	83
500	79	74	86

For the proposed and current techniques, Table 3.6 shows the intrusion detection rate in mobile node numbers. Mobile nodes vary in number from 50 to 500. Table 3.6 shows that the rate of intrusion detection is improved with the number of mobile nodes for all the techniques. In comparison with current A3ACK and CLPKM techniques, the suggested IDS-HKC method increases significantly the detection rate of intrusion [15].

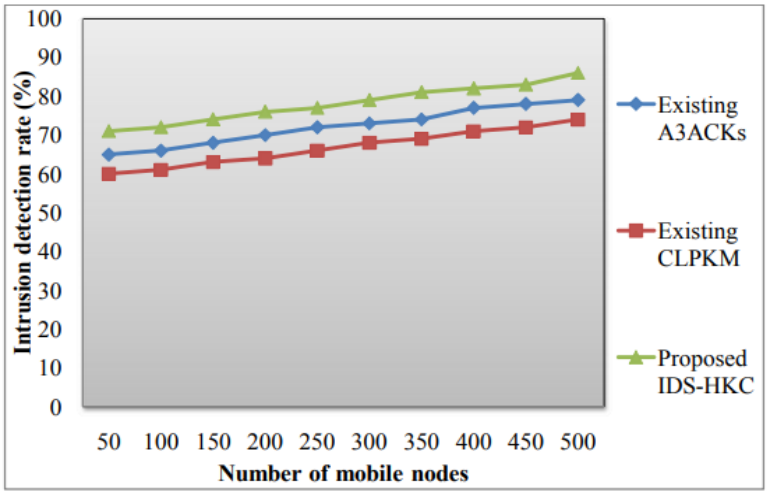

Figure 9 Estimation of intrusion detection rate

Figure 3.9 shows the intrusion detection rate of the IDSHKC technique and the current methods A3ack and CLPKM are used to conduct compare the analysis. In comparison with the current techniques the IDS-HKC method considerably increases the rate of intrusion detection. By using the cryptographic puzzle technique which is utilized to hide the traffic pattern for intruder nodes in MANET this efficient

improvement is achieved in the IDS-HKC procedure. During the cryptographic problem resolution that needs additional computing time, intrusive nodes may be identified. Therefore, when compared to current A3ACK and CLPKM techniques, the intrusion detection rate of the proposed IDS-HKC method is enhanced correspondingly by 8 percent and 15 percent.

- **Data Encryption Standard**

The Data Encryption Standard (DES) in 1972 determined that a powerful cryptographic algorithm was required to safeguard non-classified information by the National Institute of Standards and Technology (then the National Standards Office). The algorithm has to be cost-effective, widely accessible and extremely safe. NIST envisaged anything that might be utilized in a multitude of applications and accessible to the general population. They thus requested such an algorithm for public bids. In 1974 the Lucifer algorithm was presented by IBM, which seemed to satisfy most of the NIST design criteria. The National Security Agency has recruited assistance from NIST to assess Lucifer's safety. There was a fair degree of scepticism about the Lucifer's analysis at the time when many people had distrusted the NSA because of its very clandestine operations. One of the major concerns was that the main length, 128 bits initially, had been cut to just 56 bit.

It was also accused of altering the algorithm to create a "back door" through which agents may decode material without the encryption key being known. But these concerns were unwarranted and there was not ever any such backdoor. On 23 November 1976, NIST accepted the updated Lucifer algorithm as federal standard. The Data Encryption Standard has changed its name (DES). The specification of the algorithm was released in January 1977 and was extremely extensively used in a short period with the government's official support. Unfortunately, several shortcut techniques have been identified throughout time which may substantially decrease the time required to obtain a brute DES key.

As computers became faster and stronger, a 56-bit key was simply not enough big for high security applications. In 1997 the NIST abandoned its official DES approval and started to work on a replacement known as Advanced Encryption Standard due to such severe shortcomings (AES). DES is still used in large numbers by financial services and other industry across the globe to secure critical online applications, despite increasing worries about its vulnerability. RSA Data Security has supported a number of DES cracking competitions since early 1997 to underline the need for better security than a 56-bit key can provide.

In 1998, by breaking down DES in fewer than three days, the Electronic Frontier Foundation won the RSA DES Challenge II-2 challenge. EFF has utilized DES Cracker, a specifically designed computer that was created for less than $250,000. The DES Cracker's encryption chip was able to handle 88 milliards of keys per second. Recently

distributed in the beginning of 1999. The RSA DES Challenge III was won with a record-breaking time of 22 hours and 15 minutes by DES Cracker and a global network of close to 100,000 PCs. When the right key was discovered, the DES Cracker and PCs together tested 245 billion keys per second. In addition, a specialized hardware device that can search for all potential DES keys in approximately 3.5 hours may be constructed for a cost of $1 million.

This illustrates just that any moderately resourced organization may now break past DES with very little effort. The 64-bit key is used to encode and de-encode 64-bit data (although the effective key strength is only 56 bits, as explained below). The 64-bit plaintext block is used as the input and the 64-bit cipher text block is output. DES is both a block cipher and a cipher of the product, since it always works on blocks of the same dimensions and utilizes permutations and replacements in the algorithm. DES contains 16 rounds, which means that a cipher is reproduced 16 times using the main algorithm. The number of rounds has been shown to be exponentially related to the time needed to find a key using a brute force assault. The safety of the method therefore improves exponentially as the number of rounds increases. For this application, the actual implementation of DES in C is based on a simplified step-by-step description:

- **Key Scheduling**

While the DES input key is 64 bits long, the real DES key is 56 bits long. In each byte the least important (most right) bit is a parity bit and should be set such that a peculiar number of 1s in each bite always exists. These parity bits are disregarded and thus just the seven biggest bits are utilized for every byte, which gives a 56-bit key. The first step is to use a permutation called Permanent Choice 1 to pass the 64-bit key. The following table is provided for this purpose. Please note that in all following bit number explanations, 1 is the leftest bit and n is the right bit.

Table 7: Permuted Choice 1 (PC-1)

Bit	0	1	2	3	4	5	6
1	57	49	41	33	25	17	9
8	1	58	50	42	34	26	18
15	10	2	59	51	43	35	27
22	19	11	3	60	52	44	36
29	63	55	47	39	31	23	15
36	7	62	54	46	38	30	22
43	14	6	61	53	45	37	29
50	21	13	5	28	20	12	4

For example, the PC-1 table shows how bit 30 of the initial 64-bit password changes into something in the new 56-bit password. Find number 30 and note it is a part of column 5 and row 36. Remember the number 30 in the table. Add the row and column value to determine the new bit location within the key. Bit 30 is a bit 41 of the new 56-bit key, thus bit 30 is a bit 41. The original keys are not included in the table in bits 8, 16, 24, 32, 40, 48, 56 and 64. These are the unused parity bits wasted when creating the final 56-bit key. Now that the 56-bit key is available, the next step is to create 16 48-bit sub-keys, known as K[1]-K[16], used for encryption and decryption in 16 DES rooms. This process - known as the key planning - is very easy for creating sub keys:

1. Set the number of round R to 1.
2. Divide into 2 28-bit blocks the existing 56-bit key K and R L and R (the right-hand half).
3. Rotate L to the number of bits in the table below and rotate R to the number of bits left to the same number.
4. Join the new K with L and R.
5. To construct the final K[R], use Permiuted Choice 2 (PC-2), where R is the round number on which we are.
6. Increase R to 1, and continue until all 16 subkey K[1]-K[16] are available.

Here are the tables involved in these operations:

Table 8: Sub key Rotation Table

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of bits to rotate	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Table 9: Permuted Choice 2 (PC-2)

Bit	0	1	2	3	4	5
1	14	17	11	24	1	5
7	3	28	15	6	21	10
13	23	19	12	4	26	8
19	16	7	27	20	13	2
25	41	52	31	37	47	55
31	30	40	51	45	33	48
37	44	49	39	56	34	53
43	46	42	50	36	29	32

CONCLUSION:

New security concerns are created by the flexibility offered by the open media and mobile devices' cooperativeness. We need to be able to recognize these risks and take necessary action as part of rational risk management. Security issues have been quite high on MANET in recent years; the majority of research efforts have focused on particular safety areas such as the protocol securement or the establishment of a confidential infrastructure, or the detection and reaction of intruders. Intrusion detection is thus an essential component of MANET safety. An efficient and effective intrusion detection system (IDS) is thus essential for MANETs. Much study has been undertaken on this subject.

REFERENCES:

1. Boukerche, A., Turgut, B., Aydin, N., Ahmad, M., B¨ol¨oni, L. and Turgut, D., 2011, “Routing protocols in Ad-hoc networks: a survey of Computer Networks”, 55(13), 3032–3080

2. Jeenat, S. and Tasnuva, A., 2017, “Securing AOMDV Protocol in Mobile Ad-hoc Network with Elliptic Curve Cryptography”, International Conference on Electrical, Computer and Communication Engineering (ECCE), IEEE, 539-543.

3. Sagar, R. D., Chatur, P. N. and Nikhil, B. B., 2016, “AODV-Based Secure Routing Against Black hole Attack in MANET”, IEEE International Conference on Recent Trends in Electronics Information Communication Technology, IEEE, 319-326.

4. Soufiene, D., Farid, N. and Zonghua, Z., 2011, “Mitigating Packet Dropping Problem in Mobile Ad-hoc Networks: Proposals and Challenges”, IEEE Communications Surveys & Tutorials, 13(4), 658 - 672.

5. Abdelshafy, M. A. and King, P. J. B., 2016, “Resisting Black hole Attacks on MANETs”, 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 1048 - 1053.

6. Sukanesh, R. Edsor, E. and Aarthylakshmi, M., 2016, “Energy Efficient Malicious Node Detection Scheme in Wireless Networks”, IEEE, 307-312

7. Sen, J., Koilakonda, S. and Ukil, A., 2011, “A mechanism for detection of Co-operative Black hole attack in Mobile Ad-hoc networks”, Second International Conference on Intelligent Systems, Modeling and Simulation, IEEE, 338-343.

8. Mistry, N. Jinwala, D. C. and Zaveri, M., 2010, “Improving AODV Protocol against Black hole Attacks”, International Multiconference of Engineers and Computer Scientists, 2,(6), 1-6.

9. Su, M-Y., Chiang, K-L., and Liao, W-C., 2010, “Mitigation of Black-Hole Nodes in Mobile Ad-hoc Networks. International Symposium on Parallel and

November /December 2020
ISSN: 0193-4120 Page No. 387-406

Distributed Processing with Applications", IEEE, DOI: 10.1109/ISPA.2010.74, 105-113

10. Gupta, S., Kar, S. and Dhararaja, S., 2011, BAAP: "Black hole Attack Avoidance Protocol for Wireless Network", International Conference on Computer & Communication Technology (ICCCT), IEEE, 1-6.

11. Saha, H. N., Bhattacharyya, D., Bandhyopadhyay, A. K. and Banerjee, P. K., 2012, "Two-level Secure Re-routing (TSR) in Mobile Ad-hoc Networks", IEEE, 119-122, DOI 10.1109/MNCApps.2012.31.

12. Bhosle, A. A., Thosar, T. P. and Mehatre, S., 2012, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA), 2(1), 45-54.

13. Thachil, F. and Shet, K. C., 2012, "A trust based approach for AODV protocol to mitigate Black hole attack in MANET", International Conference on Computing Sciences, IEEE, 312-325.

14. Bindra, G. S., Kapoor, A. Narang, A. and Agrawal, A., 2012, "Detection and Removal of Co-operative Black hole and Gray hole Attacks in MANETs", IEEE, 3(11), 207-212.

15. Ukey, A. S. A., Chawla, M. and Singh, V. P., 2013, I-2ACK: "Preventing Routing Misbehavior in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887), 62(12), 345-353.