International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Improvement of Performance Metrics and Security of AODV Routing Protocol using Central Dogma of Molecular Biology Based DNA Cryptography

Gambhir Singh, Rakesh Kumar Yadav

Abstract: ***Mobile ad hoc network is appealing mechanization in many applications, including disaster recovery and communication systems and rescue due to the flexibility offered by the diverse network. An equivalent network, although it has been found that legitimate can operate independently, or may link to the wider Internet. A framework has been introduced in recent years operators and attackers, have used this network environment. Mobile Ad hoc Network is the main concern about dynamic routing access. Mobile ad hoc network provides several well-known protocols for routing responsive like DSR, AODV, TORA, etc. AODV can route both unicast and multicast. AODV routing protocol cannot protect against a wormhole attack. In this paper, we implement a technique of pseudo-DNA cryptography, focused on the molecular biology's central dogma. In this approach, we simulate the central dogma's transcription and translation process, and even some extra features to make it difficult to crack the resulting ciphertext and defense against wormhole attack. In the sense of ratio for packet drop, throughput and the delay between two nodes we also examine the impact of the wormhole attack on a parameter of ad hoc network.***

Keywords : Mobile ad-hoc network, AODV routing protocol, Central Dogma of Molecular biology.

I. INTRODUCTION

Mobile Ad-hoc Network [1] is a mixture of self-prepared, self-configuring movable nodes, forming an interim network with very little central control and fixed infrastructure. Each mobile node travels randomly from one place to another and operates from one node to another as a host or packet forwarding router. It is an appealing technology for several applications, include in such communications, disaster recovery, and rescue, due to the efficiency that the diverse technology offers. Such a network will run autonomously or will connect to the wider Internet.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Gambhir Singh*, Research Scholar, Computer Science and Engineering, IFTM University, Moradabad, India. E-mail: gambhirmtech@gmail.com
Dr. Rakesh Kumar Yadav, Department of Computer Science and **Engineering**, IFTM University, Moradabad, India. E-mail: rkyiftmuniversity@yahoo.com

The number of protocols Routing [9] has been implemented in recent years but it has been found that this type of framework is available to Authentic users and attackers alike. The goal is to make routing protocols adaptable to attacks to ensure secure routing is achieved.

A. Routing for mobile ad-hoc networks

Routing is the technique of sending the packets from source to goal via the most effective route is called routing. An optimal path/route is said to be based on different metrics including traffic, quantity, hops, protection, etc. The routing protocols [9] are used to reduce delays, optimize network over placement and increase energy efficiency. Routing for mobile ad-hoc networks could be generally categorized into three sections:

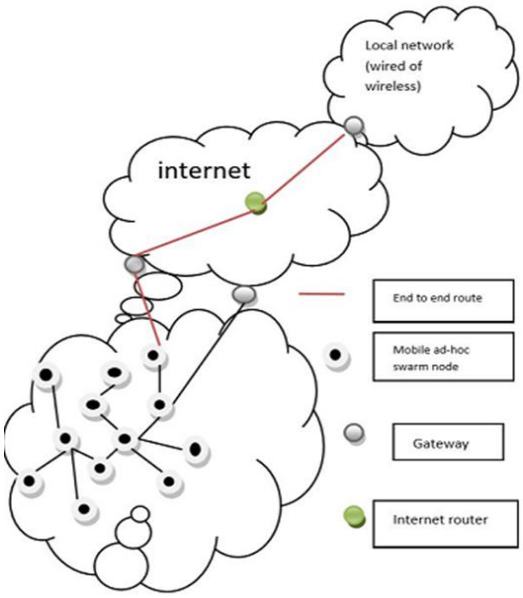

Fig.1. Architecture of Ad Hoc Mobile Networks

- Proactive or table-driven routing protocols: It also remembered as table routing [9].

There is a table in every mobile node that contains complete routing information about the topology of the network, even without it being needed. When valuable for datagram traffic, this function requires substantial power and traffic consumption signaling.

The routing tables are continually updated wherever topology changes from within a connection. Proactive protocols for large networks are not suitable, because they must carry node entries for every node. Many known table-driven protocols .like OLSR, WRP, DSDV, etc.

- Reactive or on demand routing: The reactive or on-demand is challenging routing protocol as the route has been discovered if required.
- The route discovery starts from request nodes. The node sees the path cache from starting end to destination end . if the route is not available then the process for searching begins. Mobile ad-hoc network includes several eminent reactive or on-demand protocols like DSR, AODV [17], TORA, LMR, among others.
- Hybrid Protocols for Routing: Hybrid routing combines the best feature of table-driven and reactive routing protocols. The important idea behind this routing technique is the use of a table-driven routing technique in certain parts of the ad hoc environment for certain times and on demand routing for the remainder of the router. Actions are limited to a lesser area that minimizes overhead power and delays. The adaptive technique follows to locate nodes beyond this area, as they require less bandwidth in the fast-changing network. A few belongings are as follows: ZRP, CEDAR [9], and (ZHLS), etc.

B. Mobile ad-hoc networks security aspects

Ad hoc networks are open to both legitimate users of the network [2] and malicious attackers and there are certain security risks, such as confidentiality attacks, credibility assaults and no repudiation and availability of the network.

- Authentication: A process by which user id can be verified is known as Authentication is used to verify the User Sender and Receiver identity. Firstly, before initiating contact, the service ensures that both parties are legal, that they each tend to be individuals. Firstly, for all the purposes of permitted transmission and reception, it must ensure that a mediator is not the part in the impersonation of one of the two legitimate parties.
- Confidentiality: Confidentiality [3] guarantees no release of the data/information to unauthorized users. Many encryption methods can provide secrecy, as only authorized users can view the communication and identify it.
- Integrity: This service aims to ensure the accuracy of the data provided by the agreed parties. [2] The data obtained does not include any modifications, insertions or deletions.
- Access Control: [3] The whole service is designed to control resource utilization such as the host system or program.
- Availability: [4] Accessibility includes allowing authorized users to access network services or resources. Despite malicious incidences, it ensures the survival of the network.

C. Attacks on Mobile Ad-hoc Networks

Ad-hoc network mainly contains two kinds of security attacks. There are two types of attacks; passive attacks, active attacks, and others.

- Passive attacks: Passive attacks [2] [3] [4] discover important information about the network like network node location, traffic pattern, bandwidth used, etc. This important information about the network could be used for negative attacks to come. Eavesdropping and traffic monitoring are examples of passive assaults.

Eavesdropping Attacks: Attacks of these types are also known as vulnerability attacks [3]. External or internal nodes gather information such as an encryption key, private key or node passwords in this attack they evaluate transmitted messages to identify those important network information.

Traffic Analysis [4]: The encrypted messages or network traffic can be analyzed to get some important information about the network which can be harmful in the future the attackers are using methods such as traffic rate analysis and tracking of time correlation etc.

- Active Attacks Active attacks [2] [3] [4] directly disturb the data or information by modification, fabrication, and interruption. Mobile ad-hoc network performance can decrease by active attacks because they are very harmful. These attacks generally start with internal nodes that are authorized to operate within the network. More than one group attack can be classified.

Denial of Service attack: This attack [4] involves the reduction or restriction of the legal access of the resources. Denial-of-Service (DoS) tries to crawl through the functionality of a certain node and additional features made available by the mobile ad-hoc network. Modification Attacks: In this attack, insider attackers can modify the data in the packet. For example, adjusting a routing packet's hop-count value to a lesser value. By decreasing the value of hop count a malicious node will draw further contact from the network.

Black Hole Attack: A defamatory node misguides the source node in black hole attacks [2] [4] by using incorrect information about the path and say to be the shortest path to the target node. When a path is established by the malicious user between the source node and the destination, the malicious user then misuses or discards any or all of the data transmitted through it. This is the denial of service type attack is the black hole attack [18].

Impersonation or Spoofing: In such a type of attack[3] [4], malicious users may assume, without restrictions and clear notice, the identity and rights of another legitimate user to the recipients of the impersonator's calls which have delicately taken place.

Wormhole attacks [2] [3] [4]: A compromised node over ad-hoc connections collides with a network shortcut created by such an external attacker.

By building this technique, they exploit the initial node to gain in the course of route-searching and then unleash the interference attacks later. Packages from Typically those two conspiring attackers are transferred from source to destination node consuming a wired connection to establish the very fast route alternatively if fake routes are continually maintained by wormhole nodes [18], other routes may be permanently rejected. Consequently, the intermediary nodes exist along rejected routes that cannot be part of network operations.

D. Ad-hoc on-demand distance vector (AODV)

A unicast, reactive, on-demand routing technique is the Ad Hoc on Demand Distance Vector Routing (AODV) Protocol [17]. Often recognized as the only reactive protocol, as the path is discovered where necessary. The routing detail about the active routes needs to be maintained. Only the routing information regarding the active routes must be retained.

Routing knowledge about nodes is stored in AODV [17 each node maintains a table for the next that includes the destinations it currently established route. A time-updated entry to the routing table, or for pre-specified expiry time. All nodes need to do is preserve the routing details about the active routes. Routing information about nodes in routing tables is held in AODV [17]. Every node holds a routing table next-hop, which includes the destinations it currently has a path .

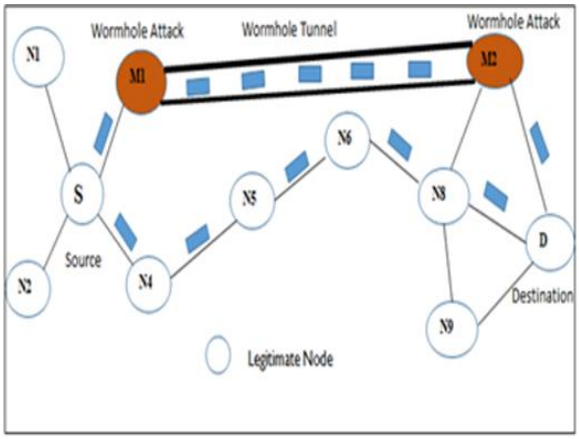

Fig.2.Wormhole Attack

E. Attacks of AODV Protocol

AODV protocol attacks are of several types [17] as well as details about each attack in the security system. A sender cannot reject the message after it has been sent and the recipient cannot dispute it after the message has been received. And it'll be possible to deny service (DoS) and AODV system security [17] by routing protocol attacks.

- **Attack the Denial of Services**

In the AODV [17], DoS attacks disrupt channel access and may result in the bandwidth of the links ' resources being wasted as well as node power. Another form of Distributed Denial of Service (DDoS) targets a network-wide use of different sources. Thus attackers create excessive circulation in ad hoc networks, DoS attacks [4] are difficult to stop and safeguard.

- **Black hole Attack in AODV**

In black hole attacks [17] [18] the illegal node misguides the initial node by using incorrect route information and claiming to have the shortest path to the end node. When a route is Established by the malicious between the initial node and the destination. Node, malicious node will then misuse or delete any or all of the transmitted data.

- **Wormhole**

DoS attacks disrupt channel access in the AODV routing protocol [17] and can cause the bandwidth of links ' resources to be wasted as well as node power. The type of Distributed Denial of Service (DDoS) is targeted at using different sources across the network. Thus attackers generate unnecessary circulation in ad hoc networks, and DoS attacks [4] are hard to avoid and defend. Fig. 2 shows detection of the wormhole. In fig.3 there is a route discovery process for AODV. The process starts with Hello,RREQ,RREP.

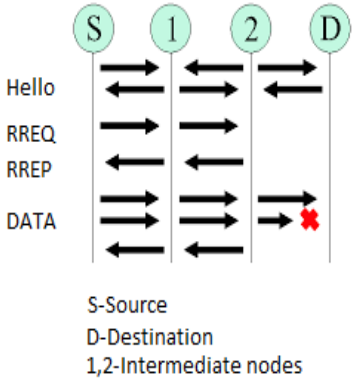

Fig.3.: AODV.Route Discovery process

F. DNA cryptography

DNA cryptography is an updated paradigm in cryptography investigation which is very encouraging. DNA could be used to compute, store and transmit information cryptography [22]. Several DNA computing algorithms are currently very strong in the problems of cryptography, cryptanalysis, and stenography. We are beginning with a new and updated cryptography scheme depend on the core dogma of molecular biology. Because this scheme facilitates various essential processes in central dogma, the pseudo-DNA cryptography program also is named. The theoretical analysis and experiments will show competence in measurement, storage space, and communication with this method; and it is immensely powerful against some attacks [23].

Adelman, The key idea is to use an amazing methodology to solve the problems which are either irresolvable on modern computers, or that require a great deal of computing.

By adopting DNA computing the Cryptographic Data Encryption Standard is easy to hack. DNA [22] enumeration is also known as molecular computing, which for massively equivalent calculation uses the inherent combination properties of DNA. Therefore the DNS enumeration presently depends mainly on DNA storage space collection and parallel computation. In a paper arguing that DNA enumeration's high-level computational capability and extremely versatile data storage media has the potential for DNA-based one-time pad cryptography [23].

Although the existing realistic implementations of one-time cryptographic pad-based systems are restricted to traditional electronic Press confine, they thought small amounts of DNA might be appropriate for a single pad to be used in PKIs.

- **Biological principles**

The central dogma of Molecular biology's shown in Fig.4 in the following diagram:

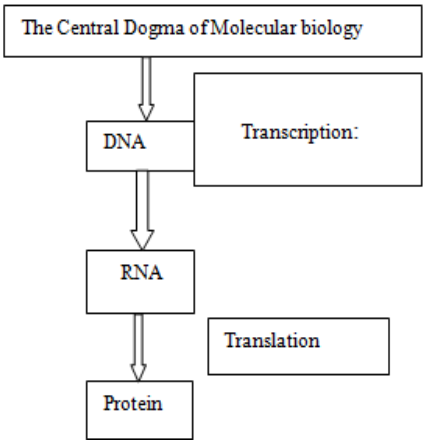

Fig.4. the molecular biology's Central Dogma

Transcription processes and splicing: A gene-forming section of DNA is read, starting with the DNA sector promoter (start). The promoter (starting position) of the DNA fragment is used to read a part of DNA that forms the gene. The stranded mRNA (Messenger RNA) sequence is transcribed into a script. The mRNA travels to the cytoplasm from the nucleus [22] [23].

Translation: The transcription of mRNA is translated in the form of amino acids [25] is incorporated as the protein. The ribosome reads the Fragment during transcription, beginning from certain three basics, after which the ribosome recognizes three essentials of mRNA at a time and turns it into a single amino acid; there are many other final bases for translational ending signatures [23] as well.

The ribosome reads the fragment during transcript, starting with certain three basics, which helps the ribosome to read three basics (codon) of the mRNA at the same time and turn them into an amino acid, as well. The pseudo-DNA encryption [is comprised of two sections, similar to the translation/splicing and transcription methods. We made a few changes to the current replication process to make it impossible to misinterpret the text of understanding. The initial characteristics of the introns are their start and end codes which allow you to devise the introns relatively easily. This has moved to another method, in which both start codes and pattern codes have defined the introns. The feature codes are non-perpetual patters showing which frame parts to delete and which sections you will retain. The introns are now dispersed, so it makes it difficult to comment about them. If the introns ' length can be determined by start and pattern codes, end codes are not needed.

The information is kept in binary form for A and can be translated into DNA form using digital DNA coding as shown in the table1.

Table-I: DNA digital Coding

Binary Values	Nucleotides of DNA
0	A
1	C
10	G
11	T

A understands the initial codes (introns ' starting codes) and the sequence code(s) (the frame parts to be removed and which parts to be maintained) of the intruder and therefore knows where the introns should be retrieved in DNA type. So the following can be represented as 2 sections

1. A searches the DNA kind of data to identify the introns. This tracks the positions of the introns and cuts the introns accordingly. This translates the DNA data type into mRNA data form [24].
2. A converts the data type mRNA into data form protein according to the table of genetic code (20 amino acids are made from 61 codons) [25].

II. LITERATURE SURVEY

An effective low-frequency broadcast authentication protocol overhead computation and communication.TESLA uses mainly symmetric cryptographic functions, but asymmetric from clock synchronization and delay key disclosure is achieved. In TESLA, For secure authentication sender or receiver must buffer some messages. TESLA's weaknesses are; first, it requires expensive digital signatures to validate the initial packet, and second, it exposes a link to every packet that takes so much time to send and receive. TESLA is susceptible to DoS attacks since malicious nodes may determine the status of buffer overflow [19].SEAD founded on the DSDV-SQ variant of the Sequenced Distance Vector (Destination) protocol. This protocol copes with routing information changing attackers and also with replay attacks. Instead of expensive asymmetric cryptography operations, using one-way hash chains is cheap. To avoid the attackers, two different approaches are used for authentication of messages. SEAD is not tackling wormhole attacks [8].CONFIDANT based on DSR as an extension CONFIDANT allows the monitoring and reporting of route setting that prevents nodes from being misbehaved. It uses as protection method Control, Reputation Program, Path Manager, and Trust Manager. It is the reputation-based detection system. CONFIDANT is susceptible to hacking [20].Clarified their DNA-based single-pad encryption scheme. They claimed that "For public infrastructure services (PKI), DNA could use a large individual pad (PKI).DNA cryptography on the common PKI framework is implemented, the investigators claim that they could interpret the similar method implicit in PKI but use the intrinsic equivalent processing DNA bonding computing Principles for public and private key encryption and decryption. Essentially, the algorithm for transaction coding may now be harder than that used in traditional coding methods [23].The DSR routing protocol depends on this. CORE promotes node collaboration by tracking node collaboration and reputation process.

The scheme CORE is resistant to attacks carried out using the system itself: no negative ratings are distributed. Yet CORE does not discriminate against nodes that malfunction and misbehave. Malfunctioning cannot regain its credibility when it recovers from the question of temporality [21].A safe routing protocol called SANE-DNA based on DSR and on-demand routing protocol [10] has been implemented. This protocol is based on one-time -pads pseudo-DNA cryptography. SANE-DNA uses symmetrical encryption. It gives honesty, repudiation, and confidentiality.

SANE-DNA cannot deal with an autonomous node. Securing routing protocol is a compatible extension with several existing reactive techniques like AODV. In SRP, during the path searching process, the initiator will detect and discard false responses. SRP prevents attacks that interrupt the path searching process and guarantees accurate location information of the network. The process of route discovery and guarantees that topological information is accurate [12].
Some ad hoc routing protocol expanded upon request. SAR needs nodes that share the same confidence level as a private key. SAR [14] improves routing through Digestive and symmetrical hash encryption methods.
The signed hash digests confirm the truthfulness of the data while the encryption of the packet guarantees confidentiality [14].It gives a secure, constructive topology experiment, and can be used as an individual protocol or as a share of a hybrid scheme in combination with the on-demand protocol. SLSP requires that every node transmits its public key periodically to nodes beyond the area, to operate effectively without the node of central key management authority. However, it frequently transmits signed HELLO messages to its neighbors with its physical address and Internet Protocol address pair. [15]. SLSP May function within networks where topology and membership are constantly changing. SLSP is vulnerable against specific attackers and can change the network-wide and local topology discovery continuum.
To ensure neutral traffic control is relayed even when DoS attacks are clogged, SLSP participates in a round-robin system [15].The Analyzing security of Authenticate Routing Protocol (ARAN) is proposed by [5] which is based on AODV [9] introduces the Integrity of message, authentication, and non-repudiation. ARAN [5] protocol can detect and protect against malicious attacks using the third party. ARAN protocol [5] uses two stages of security i.e. simple mode and optimized mode. Simple mode is necessary whereas optimized mode provides stronger security but it is an overhead that is not suitable for mobile node because the mobile node contains limited processing and battery power. ARAN [5] uses a cryptographic credential for non-repudiation and authentication [2]. ARAN has a high computational cost for route discovery due to asymmetric cryptographic operation and large routing packets. ARAN [5] is also vulnerable selfish nodes and a selfish node is an authenticated node then ARAN is incapable of detecting these attacks. ARIADNE [6] cannot avoid wormhole attack and attack through cache poisoning. Second, the key swap is very difficult. Secure On-Demand Distance Vector Routing is a secure routing technique with high efficiency this helps to improve in AODV [9][16] protocol. The security measures like user verification, hash chain, and digital signature enhance safety but increase the computational burden and time delay which degrade the performance of routing protocol so there is a scope to improve in SAODV [13].In Adaptive-SAODV certified Public Key Ownership enables authentication of all in-transit routing packets by intermediate nodes. It is loop-free and uses trust party arrangements that are not secure [7].The author has proposed Trust-Based technique. TAODV is a reactive routing protocol which is an improved version of AODV [9] based on portable node trust worth. TAODV [11] needs only two modifications in the existing AODV protocol. First, Trust Request(TREQ) and Trust Reply(TREP) control packets; second, Revised extended Four new fields routing table; Useful events; adverse events; track status; opinion. In this method, a safe route between the initial node and the destination explained by measuring the participating confidence value of the nodes in the route setup process. It is based entirely on the confidence value of nodes [11].The author has proposed a method based on Cryptographic Authentication Mechanism to study a balance between higher safety and efficient network. The proposed method to secure AODV [9] uses the hash technique for message authentication. This technique provides fast verification and authentication of message and node authentication due to the absence of asymmetric key cryptographic operation. This technique minimizes the time lag and overhead network search packet as compare to SAODV [13].

III. PROPOSED DNA CRYPTOGRAPHY MATHOD

We use OTP (One Time Pad) key generation in our implemented algorithm. OTP is a procedurally generated key used for encryption and decryption only once, which is altered for further encryption. As an encryption and decryption tool, XOR also is used.

A. Key Generation

The DNA sequence of nucleotide known as the DNA-OTP key represents the OTP key produced. The main production process for DNA-OTP as follows:

1. Read the text input message. (2) Compute the length of the message (L) and randomly generate the DNA nucleotide sequence equal to the length of the message. (3) Apply the process of annealing to the DNA-OTP key to create a double helix DNA-OTP key by using the base-pairing rule to pair A to T and C to G, as shown in. (4) Apply the process of transcription to convert double helix DNA-OTP key to mRNA sequence by converting every T in DNA-OTP key to U in mRNA. (5) The final step, apply the process of translation to mRNA codons, using a standard table which converts RNA into amino acid to create a protein key.

B. Encryption

The suggested algorithm uses an encoding method for the numerical operation XOR. The message is transformed into ASCII value after that calculate the binary value (2). The generated protein key is transformed into ASCII value then transformed into a Binary value. (3). Apply XOR process between the binary of the message with the binary of the protein key, and described by the equation below, where the protein key is K,
The message is M and the resulted cipher text is C.(4) Finally, cipher text in Binary format is converted to DNA format by using Table I.

C. Decryption

The message can be recovered by using the arithmetic operation XOR as a decryption technique. XOR operation is used because if XOR operation applied twice, the result is the message again e.g., XOR [K, XOR (K, M)] =M, where protein key K and message M.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

In this example, the inner XOR process represents encryption, where the decryption is the outer XOR operation. Thus, XOR operation applied for both ends for encryption and decryption too. The steps of the decryption process are as the following: 1. The cipher text in DNA format is converted to Binary format by using Table1. 2. The generated protein keys are transformed to ASCII value after that transformed into Binary value. 3. Apply XOR process with the binary of the encrypted message and the binary of the protein key, as described by the equation below, where the protein key is K, the cipher text is C and the resulted message is M. 4. Finally, the message in binary format is converted into ASCII code than to text message.

IV. RESULTS AND DISCUSSION

The tests are performed over two square kilometers with 25 nodes spread. It uses the AODV routing protocol. The first experiment is conducted without malicious nodes and the second experiment with 20 percent of the nodes being malicious. The third experiment is proposed with AODV. The results contrast between the three studies is seen in Fig. 5 to 9. The outcome value of the above-mentioned contrasts is shown in Table II through IV. From fig.5 it is found that if 20 percent of malicious nodes in the network throughput is decreased by 58.63 percent. When suggested pseudo-DNA based cryptography is applied on AODV routing dramatically improves the performance in a malicious environment achieving a result that is 5.05 percent lower than the performance obtained by AODV in a non-malicious context. System time. It makes the time assessment equal. The following table shows the wormhole attack between two colliding malicious nodes by AODV.

Table II: Throughput in bits/sec

Simulation time (in a sec)	AODV	AODV with wormhole attack	DNA
90	1822203	274132	1773914
180	1666133	400081	1591491
270	1683251	721772	1600771
360	1760596	774880	1701088
450	1760596	818632	1335115
540	1601023	600280	1486710
630	1626348	793182	1556903
720	1671467	782567	1622994
810	1754683	698013	1634136

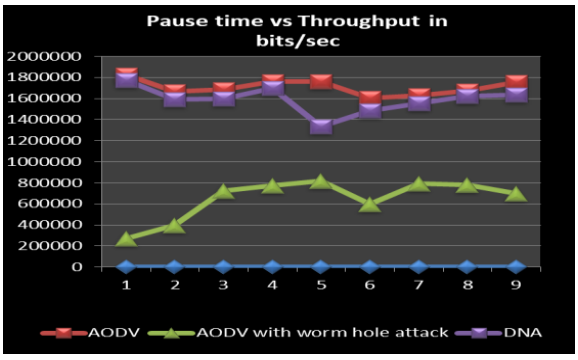

Fig.5. Throughput in bits/second

Table-III :Packet drop ratio

Simulation time in second	AODV	AODV with wormhole attack	DNA
90	48	16	18
180	55	25	27
270	45	19	20
360	52	18	19
450	56	19	20
540	39	11	12
630	51	27	28
720	64	56	59
810	47	41	43

Table -IV:End to End Average delay

Time duration (in a sec)	AODV	AODV with wormhole attack	DNA
90	0.007232	0.0080638	0.00785
180	0.005291	0.0094155	0.008994
270	0.006585	0.0091506	0.008702
360	0.007233	0.008773	0.008476
450	0.008095	0.0080998	0.007495
540	0.008002	0.008214	0.007628
630	0.008245	0.0086875	0.008317
720	0.008243	0.0088372	0.008581
810	0.007987	0.0106493	0.009918

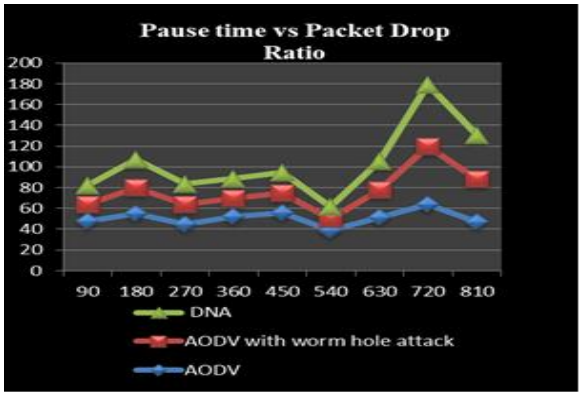

Fig.6.Packet drop ratio

Fig.6 shows the number of drop ratios for packets in the path searching process. From the figure, it is found that if 20 percent of malicious nodes, the amount of ratio for packet drop is three times greater.

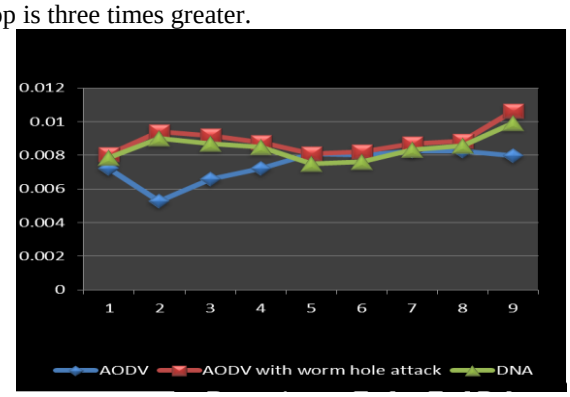

Figure. 7: End to End Average Delay.

Fig.7 provides a comparison of the delay between two ends estimated in seconds saluted by the standard and wormhole. In the case of an attacker, it has seen which creates a wormhole attack; the delay between two ends is more variable. Compared to the AODV, the proposed AODV reduces the delay between two ends by 5.1 percent in the malicious environment.

A. Analysis of Pseudo DNA Cryptography

Suppose that the DNA information type D is n long. There are k introns, the average length of which is m. The mRNA information type D' is then n-k*m long. The protein type of Information D "has a length of (n-k*m)/3 as one codon (include 3 nucleic acids) can typically be converted into one amino acid. Both encryption and decryption take running time O (n).

B. Evolution

In the Linux environment, A core to duo (2.2 GHz)/2GB system was used as an encryption and decryption algorithm for the efficiency of the research in C language (UNIX).
To check the device robustness, we have chosen 4 separate plain texts of the increased size of each encryption/decryption cycle, which is 10 times higher and takes account of the average time.To test the output of the software, we used a highly distracted text which includes short, long text, strictly alphabetic and text combinations of alphabets. The various texts mentioned in Table-V.

Table-V:Performance of the application with messages of different content

Experiment	Explanation	No. of Characters	Recovery of message
Test1	alphabetic and digital characters	52	Yes
Test2	Non-alphabetic and non-digital characters	100	Yes
Test3	Grouping of Characters	75	Yes
Test4	Grouping of Characters	125	Yes

We also have redundancies (tags and separators) added. The current key data depends on the size of the introns, but it is approximately less than half of the size of the introns, including redundancy (see table-VI). There is also a list of encoding and decrypting times indicating the efficiency of the algorithm.

Table-VI: Performance of the application with messages of different size

Tests	Size of Plaintext (Bits)	Length of Cipher Text	Size of Key (with redundancy)
Test1	10	51	100
Test2	100	396	715
Test3	1000	3521	5220
Test4	10000	36212	48140

Logoff (Length) denoted by numeric values

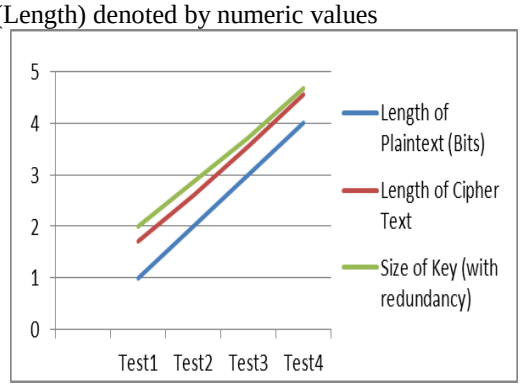

Fig.8: Performance of the application with messages of different size

Table-VII: Encryption and Decryption time

Dataset	Encryption Time (ms)	Decryption Time (ms)
Test1	255	429
Test2	259	433
Test3	299	484
Test4	1293	1399

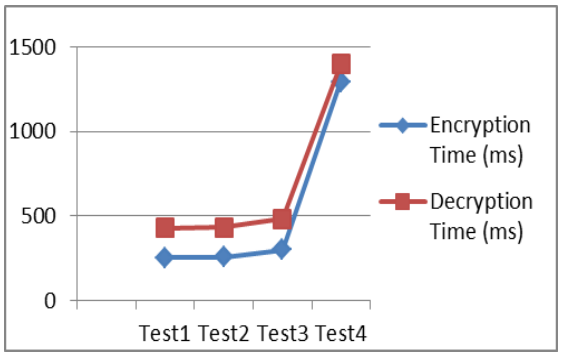

Fig.9. Encryption and Decryption time

V. CONCLUSION

Previously, the research done on security issues, i.e. the mobile ad-hoc network attack was dependent on AODV reactive protocol for routing. Under the AODV technique, various types of attacks are analyzed and their results are elaborated by specifying how these attacks interact with mobile ad-hoc network's efficiency and protection. It has been found that routing protocols are threat-oriented if the schemes fail when there is a new attack. TESLA is prone to DoS occurrences, as attacker's nodes may produce buffer overflow. SEAD struggles to tackle the wormhole attack. CONFIDANT is weak enough to spoof. In CORE, when it recovers from a temporal problem, malfunctioning cannot rebuild its reputation. SANE-DNA can't handle greedy nodes. ARIADNE cannot avoid wormhole attack and attack through cache poisoning. Second, the key swap is very difficult. Link cache poisoning, lack of authentication for link repair messages, is caused by SRP.SRP doesn't resistant wormhole attacks ARAN is vulnerable selfish nodes and selfish nodes are authenticated nodes otherwise ARAN cannot detect these attacks.

SAR ensures credibility and confidentiality of communications this is perhaps not the shortest path discovered hop-count route. In Adaptive-SAODV (Secure On-Demand Distance Vector Routing) certified public key ownership allows for the validation of all in-transit packets by midway nodes. Adaptive-SAODV is loop-free adaptive uses insecure trust party arrangements. In TAODV [path configuration is insufficient to make a safe path. The disadvantages of AODV Based on Cryptographic Authentication Mechanism are The hidden key is a costly process between any two nodes and it cannot verify and authenticate the RRER message. We suggested a method of pseudo-DNA cryptography on the AODV routing protocol is based on the core molecular biology dogma. In this approach, we simulate the core dogma's transcription and translation mechanism and new features OTP to make the resulting cipher text unbreakable. We suggest a procedure of pseudo-DNA cryptography on the AODV technique for routing that is based on the core molecular biology dogma. In this approach, we simulated the core dogma's transcription and translation mechanism and new features to make the resulting cipher text unbreakable in AODV to wormhole nodes and also improved the metrics like Throughput, Packet drop ratio and end to end average delay. Our research shows that the approach can be effective against many attacks. This approach will also be very successful in computing. The time taken in the process of encryption and decryption will be low, which will be very good to enhance the security in mobile ad hoc networks.

REFERENCES

1. C. E. Perkins (Ed.), Ad Hoc Networking, Addison-Wesley Longman, 2000.
2. L. Zhou, Z. J. Haas. Securing Ad Hoc Networks. IEEE Network, 13(6): 24-30, Nov/Dec 1999.
3. G. Jose Moses, Prof.P.Suresh Varma, N.Supriya, G.NagaSatish. Security Aspects and Challenges in Mobile Adhoc Networks, I. J. Computer Network, and Information Security, 2012, 6, 26-32 Published Online June 2012 in MECS (http://www.mecs-press.org/)
4. CH.V. Raghavendran, G. Naga Satish, P. Suresh Varma, Security Challenges and Attacks in mobile ad-hoc networks. I.J. Information Engineering and Electronic Business, 2013, 3, 49-58 published online September 2013 in MECS (http://www.mecs-press.org/)
5. B. Dahill, B. N. Levine, E. Royer, C. Shields, 2002, "ARAN: A Secure Routing Protocol for Ad-hoc Networks", UMass Tech Report 02-32.
6. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc.8th ACM Int'l. Conf. Mobile Computing & Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.
7. Yi, S., Naldurg, P., Kravets, R.," Security aware ad-hoc routing for Wireless networks," Proc.Of the 2nd ACM International Symposium on Mobile Adhoc networking and computing (Mobi -Hoc'01), pp.299-302, 2001.
8. Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.
9. C.-K. Toh, Ph.D., Ad Hoc Mobile Wireless Networks: Protocols and Systems Publisher: Prentice-Hall, December 03, 2001
10. K.Verma,Mayank Dave,R.C.Joshi, "Securing Ad hoc network with DNA Cryptography "at the IEEE conference on computers and Devices for Communication(CODEC006),pp781-, Dec.2006.
11. A.Menaka Pushpa, "Trust-Based Secure Routing in AODV Routing Protocol", IEEE 2009.
12. P. Papadimitratos, Z. J. Haas, and P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. Draftpapadimitratos –secure –routing - protocol- 00.txt, Dec. 2002.
13. 13. Davide Cerri, Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE Communication Magazine, Pp. 120-125, 2008.
14. Yi, S., Naldurg, P., Kravets, R., "Security aware ad-hoc routing for wireless networks," Proc. Of the 2nd ACM International Symposium on Mobile Adhoc networking and computing (Mobi -Hoc'01), pp.299-302, 2001.
15. Papadimitratos, P., and Haas, Z., "Secure link-state routing for mobile ad-hoc networks," Proc. Of Symposium on Applications and the Internet Workshops (SAINT'03), pp.379-383, 2003.
16. Preeti Sachan and Pabitra Mohan Khilar, "Securing AODV Routing Protocol in MOBILE AD-HOC NETWORK Based on Cryptographic Authentication Mechanism," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.
17. C.E. Perkins and E.M. Royer. Ad hoc on-demand Distance Vector routing, mobile Computing systems, and applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, 1999, p90 - p100.
18. Abusalah, L., Khokhar, A., Guizani, M., "A survey of secure mobile Ad-Hoc routing protocol", Communications Surveys & Tutorials, IEEE, Vol.10, No.4, pp.78-93, Fourth Quarter 2008.
19. A.Perig, R.Canetti "The TESLA Broadcast Authentication Protocol", Internet draft 2000.
20. Buchegger, J-Y Le Boudec, "Performance analysis of CONFIDANT Protocol", in Proc. of Mob hoc 2002.
21. P.Michiardi and R.Molva, "Core Collaborative Reputation Mechanism to Enforce node cooperation in Mobile Ad hoc Networks" In Proc.of IFIP Communication and Multimedia Security Conference 2002.
22. Sherif T. Amin, Magdy Saeb, Salah El-Gindi, "A DNA-based Implementation of YAEA Encryption Algorithm," IASTED International Conference on Computational Intelligence (CI 2006), SanFrancisco, Nov. 20, 2006.
23. Ashish Gehani, Thomas LaBean, and John Reif. DNA-Based Cryptography. DIMACS DNA Based Computers V, American Mathematical Society,2000.
24. A. K. Verma, Mayank Dave, R.C. Joshi, "Securing Ad hoc Networks Using DNA Cryptography", IEEE International Conference on Computers and Devices for Communication (CODEC06), pp. 781-786, Dec. 18-20, 2006.
25. Dominik. Heider and Angelika Barnekow, "DNA-based watermarks using the DNA-Crypt algorithm", Published: 29 May 2007 BMC Bioinformatics 2007, 8:176 doi: 10.1186/1471-2105-8-176, http://www.biomedcentral.com/1471-2105/8/176, © 2007 Heider and Barnekow; licensee BioMed Central Ltd.

AUTHORS PROFILE

Gambhir Singh received his B.E. degree in Computer Science and Engineering from Krishana Institute of Engineering and Technology,Ghaziabad in 2003.M.Tech degree in Computer Science and Engineering from hobhit University,Meerut and pursuing Ph.D. in Computer Science and Engineering from IFTM University Moradabad.Currently, he is working in the Department of Computer Science and Engineering of H.R. Institute of Technology,Ghaziabad; He has 15 years of teaching experience. He has published 5 research papers in International Journal and 2 research papers in National and International Conferences. He has attended 7 seminars and workshops. His areas of interests are Network Security, MANETs, Algorithms,and Computer Networks.

Dr. Rakesh Kumar Yadav pursed Bachelor of Technology from Utter Pradesh Technical University, Lucknow ,India, Master of Technology from Singhaniya University Rajasthan and Ph.D. from IFTM University, Moradabad. He has also served at Pant Nagar University of Agriculture & Technology. He is working as an Assistant Professor in Department of Computer Science & Engineering, IFTM University, Moradabad since 2007. He has published more than 19+ research papers in reputed international journals and conferences. His main research work focuses on Biometric, Image Processing, Computer Vision, Soft Computing and Artificial Intelligence. He has 13+ years of teaching experience in higher education.