Study of Attacks in MANET, Attacks on AES, Cryptographically Generated Addresses (CGAs) Methods and Possible Alleviation in IPV6 over MANET Area

Kavita Tukaram Patil
Research Scholar, CSE Department
SSBT's COET Bambhori
Jalgaon, India

Manoj E. Patil
Asst. Professor, CSE Department
SSBT's COET Bambhori
Jalgaon, India

ABSTRACT

The mobile ad hoc network (MANET) has attracted a lot of attention due to the characteristic of an infrastructure-less construction and multi-hop communication. In MANET, security is major issue, hackers has aimed to disrupt security in the form of IP spoofing or to produce a forged route. In the advancement of networks to IP version 6, appreciating the same protocol would guarantee the achievement and portability of MANETs. Two benefits of approving IPv6 are improved support for security and mobility. To accomplish these goals an innovative mechanism called Cryptographically Generated Addresses (CGAs) were announced. CGAs were primarily comprised in SEcure Neighbor Discovery (SEND) protocol to guard against IP address spoofing and attacks. In this review paper, attacks in MANET, attacks on AES, and various CGA methods are studied. Though, the CGA is hopeful security technique for use with IPV6 addresses it still exhibits vulnerabilities and weaknesses if, used with SHA-I(secure Hash algorithm) algorithm. It is yet prone to privacy related attacks. So, use such method that can be secure and efficient to CGA in IPV6 over MANET area. This paper provides necessary solution to resolve these problems.

Keywords

MANET, AES Algorithm, CGA, blackhole attack, IPV6.

1. INTRODUCTION

MANET is the new growing technology which supports users to converse without any corporal infrastructure nevertheless of their geographical location, that's why it is sometimes referred to as an infrastructure less network. Subsequently the network is distributed, all the network activities contain defining the topology and conveying the messages must be accomplished by nodes themselves. There is multi-hop routing in MANET. It means no default router is offered. Every node acts as default router and sends packets to each other for sharing information. Device in MANET should be proficient to detect the availability of other devices and achieve necessary set up to make possible communication and sharing of data and service. Ad hoc networking permits every device to maintain the associations with the network and also can easily join and eliminate devices to and from the network.

The networks can be worthwhile in a wide variety of circumstances, but locating them up and organizing services on them is a difficult task, even for experienced users. Due to mobility of nodes, threats from conveyed nodes inside the network, restricted corporal security, scalability, dynamic topology and decentralized management MANET is more susceptible than wired network and is more liable to malicious attacks [1].

To provide security the internet protocol version 6 if valuable protocol. Cryptographically Generated Address (CGA) provide necessary authentication to the IPV6 addresses CGA allows the address owner to attest address ownership by binding the public key signature to and IPV6 address. To secured CGA, here the AES algorithm is introduced. However, MANET has many applications, including ad hoc audio/video conferencing through wireless sensor networks, network robots, campus ad hoc learning tools, emergency rescue communication networks, defense tactical communications, and so on. Figure 1 represents the architecture of MANET; each mobile device can communicate with any other device in the network within the particular range.

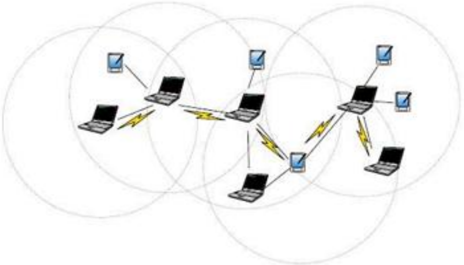

Figure 1. Architecture of MANET

1.1 Need for Ad-hoc Networks

- To established backbone infrastructure and fixed access points is not all the time feasible
- Infrastructure may be missing in a devastation spot or clash zone
- Infrastructure may be unusable for short-range radios; Bluetooth (ranges10m) [1].

Ad hoc networks:

- Can work without backbone infrastructure support.
- Are trouble-free to arrange.
- Useful when infrastructure is absent, damaged or impractical [2].

1.2 MANET challenges

While designing superior wireless ad hoc network, different challenges should be considered and are as follows:

Dynamic Topology

There is facility to travel nodes in casual manner. Consequently, the topology changes. So, it burdens for the dynamic configuration on network.

Limited Bandwidth

As wireless networks have limited bandwidth. In an ad hoc network, it is supplementary because there is absence of backbone infrastructure or multiplex higher bandwidth is also not available.

Routing

The routing in MANET is very complex. Many factors are responsible for this jumble like selection of routers, finding the routing path, topology and protocol etc.

Limited security

In MANET any node can join or leave the network at any time due to random topology. The network is more susceptible to various attacks. Mobile ad hoc networks are more exposed. As by design any node should be able to join or leave the network at any time [1] [3].

Security in MANET

Security is cause for concerning in an ad-hoc network.

- To ensure user about nobody is interfering on the traffic promoted by a node.
- To ensure the receiver is authenticated person who claims to be?
- The necessities for authentication, integrity or confidentiality are the equal as for numerous other public communications networks.
- Cryptography: We unable to trust with means of communication [4]

1.3 Motivation

As MANETs are widely applicable in Military communication, Automated Battle fields, Sensor Networks, E-Commerce, Vehicular Services, Home and Enterprise Networking, Educational applications, Environmental applications and Home applications, the security is major issue because MANET is vulnerable to different types of attacks. IPV6 is useful protocol which provides high security. CGAs were mainly planned to demonstrate address ownership in IPV6. It can attach the owner's public key to the generated address to advert stealing of existing IPV6 address. The AES algorithm is one of the best encryption algorithm which have excellent security, low resource consumption and can resist against different types of attacks.

1.4 Objectives

Objective of the proposed research are:

- Instead of SHA-I algorithm in CGAs techniques use AES algorithm as AES has high speed, excellent security and low resource consumption.
- To develop the security that can obtain optimum performance like using minimum resources forward the data packets within less than their time deadline.
- Improving efficiency by avoiding collision.
- Detect and Prevent attacks on AES.

In this section I introduction of MANET is described. In the section II the literature survey regarding Cryptographically Generated Addresses (CGAs) techniques that have future prediction is presented. The section III, titled, modifications, describes the modification made in CGA and AES algorithm. The proposed system is described in section IV. Section V describes the conclusion.

2. LITERATURE SURVEY

2.1 Internet Protocol Version 6

In MANET security has major issue; so to provide better security Internet Protocol Version 6 (IPv6) is very valuable protocol. To work well IPV6, the standard is published by the Internet Engineering Task Force (IETF) in 1998. The IPV6 is measured as backbone to the modern internet and is projected to switch the IPV4. It has capability to expand and its growth through recent large scale deployments. Therefore it is often mentioned as “next generation Internet”. For authentication and encryption among host the IPSec security protocol is inserted into the IPV6 specification. Due to the IPSec security assembled in security framework the data traffic is protected between hosts. It delivers end to end security framework efficiently. It is layer 3 best effort transport protocol. Expansion from IPV4 to IPV6 contains changing IP address from 32 to 128 bits, simplified header format, support for extension, flow labeling capability, increased privacy and authentication extensions [5].

IPv6 Overview

IPv6 has the following different features:

- Significantly better address space.
- To remain routing table small and proficient backbone routing, globally unique and hierarchical addressing, based on prefixes rather than address classes.
- Accompanying protocols are there and facility for encapsulation IPV6.
- Network interface can auto configure.
- Can easily switch from IPv4 as has alteration methods.
- In preference to broadcasting supports superior multicast routing.
- Facility for class of service to differentiate types of data.
- Incorporated authentication and encryption.
- Compatibility methods to communicate and coexist withIPv4 [5].

2.2 Cryptographically Generated Address

Identity is one of the most important aspects within the internet. It facilitates controlling user activity and access to the network in order to improve network visibility and thus improve network security. It plays a central role in the development of the Future Internet. IPV6 represents a considerable improvement compared to the previous version, IPV4. In IPv6, a public signature key can be tied to an IPv6 address and the significant IPv6 address is known as Cryptographically Generated Address (CGA). It has supplementary security protection mechanism to discover the IPV6 neighborhood router, and permits the user to supply a “proof of ownership” for a particular IPV6 address. This is a key distinguisher from IPV4; it is unattainable to fit this functionality to IPV4 as it has 32-bit address space restriction [6].

Cryptographically Generated Addresses (CGAs) were first planned in order to offer the necessary authentication for IPv6 addresses. CGAs are IPv6 addresses where the interface identifier (ID) segments which is the 64-rightmost bits of IPv6 address and the address owner’s public key has a cryptographic hash to custom ID and supplementary auxiliary parameters. To sign messages sent from that address, the address manager uses a consequent private key. In this way, the CGA technique enables the address owner to attest address ownership by binding the public key signature to an IPv6 address [6]. The availability, confidentiality, integrity, authentication and non-repudiation are goals of MANET. The routing protocol should be robust against change in topology and malicious attack to gain the availability. When routes are constructed the topology information do not required confidentially and non-replication protection. To achieve the goals like availability, authentication and integrity CGA is very useful in MANET. In MANET use of CA is not feasible because it cannot assume that a node will be always reachable by all other nodes [7] [8].

CGA offers three main advantages:

- Self-certified i.e. no third party (like Certified Authority) or additional security infrastructure is needed.
- It makes spoofing attacks against, and stealing of, IPv6 addresses much harder.
- It allows for messages signed with the owner's private key.
- It does not require any upgrade or modification to overall network infrastructure [6].

Limitations of CGA:

- Computational time necessary to generate CGAs.
- Not complete security solution it still exhibits weaknesses and vulnerabilities to threats.
- There is no guarantee that CGA address was created from appropriate node [6].

2.3 Advanced Encryption Standard

Cryptography is the art and science of creating secret codes. Although in the past it referred only to the encryption and decryption of massage along with the secret key. Today, it is mentioned as three distinct mechanisms; symmetric-key encipherment, asymmetric-key encipherment and hashing. For sharing the data, security accomplishment is performed. To encrypt the data AES algorithm is most significant standard for block ciphers because AES provide strong encryption and has been selected by NIST as Federal Information Processing Standard in 2001 and in 2003 the US Government announced that AES is secure sufficient to protect classified information up to the top secret level. The Advanced Encryption Standard (AES) selected by Rijndael is a procedure to encrypt data and is useful to change the data according to composite algorithm refer as cipher. As encrypted, the data is unable to read if a key is not used to decrypt it. AES is an iterated block cipher with a fixed block size of 128 and variable key length i.e. key sizes 128,192 and 256 bits depends on number of rounds.

The AES has fast speed and very low resources consumption. The AES in CGA entails the high security. By minimizing collision it can improve effectiveness. It has feature to resist various attacks, speed and code trimness on different platforms. It has trouble-free design [9]. The neighbor discovery protocol helps to communicate between neighboring nodes in mobile IPV6 environment and can be provided with secures function by including the RSA signature options and CGA parameters option but, the SEND protocol unable to provide confidentiality of ND Massage. To provide confidentiality of SEND protocol AES algorithm can be used with symmetric key without certification authority or any security infrastructure [10] [11].

AES operates on a 4 × 4 column-major order matrix of bytes. Most AES calculations are done in a special finite field. The AES cipher is specified as a numeral of repetition of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of numerous processing steps, together with encryption key. A set of reverse rounds are useful to transform cipher text back into the original plaintext using the same encryption key.

1) KeyExpansion round keys are derived from the cipher key using Rijndael's key schedule.
2) InitialRound
   - AddRoundKey each byte of the state is combined with the round key using bitwise XOR.
3) Rounds
   - SubBytes a non-linear substitution step where each byte is replaced with another according to a lookup table.
   - ShiftRows a transposition step where each row of the state is shifted cyclically a certain number of steps.
   - MixColumns a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4) AddRoundKey
5) Final Round (no MixColumns)
   - SubBytes
   - ShiftRows
   - AddRoundKey

2.4 Attacks in MANET

MAC layer Attack

Jamming Attack

It is the special class of DOS attacks. It is originated by malicious node after determining the communication frequency. It sends signal on that frequency so that error free receipt or is delayed. Jamming attacks also avoids reception of appropriate packet [12] [13].

Hamid A. and Ben Othman J. [14] proposed method for detection of jamming attack by the measurement of error distribution. In this approach the jamming detection is depends on the measure of statistical correlation. The correlation is nothing but a measure of the association between two random variables. In this approach the jammer sends only when valid radio activity is signal from its radio Hardware. Limitation: - This method detects DOS attack at MAC layer only.

Network Layer Attack

Wormhole Attack

This type of DOS attack happens on network layer. In this, malicious node collects packets from some location in the network and bridges them to another location in the network, where these packets resent into the network. It is also referred as tunneling attack. This tunnel between two colluding attackers is denoted as wormhole. It is established through wired link or wireless link. The two or more nodes may work together to compress and altercation massage between them along existing data routes [12] [13].

Yih-chun Hu Adrian Perrig [15] proposed approach geographical leashes and temporal leashes. A leash is nothing but information packet to restrict its transmission distance. The geographical leashes confirm that the receiver must be within certain distance from the sender and temporal packet leashes set a bound lifetime of packet which adds constraints to its travel distance.

Limitation: - Limitation of GPS Technology and all nodes requires tightly synchronized clock.

Blackhole Attack

In this, an attacker uses routing protocol. If attacker wants to interrupt the packet of any node, it publicizes itself as shortest path from that node. When attacker accepts any request which it has to route for destination node, it generates reply of very short route. The attacker's (malicious node) reply reaches at the source before reply from actual destination node, a fake route created once the malicious node get inserted into between interactive nodes and it can do anything with packet passing between them [12] [13].

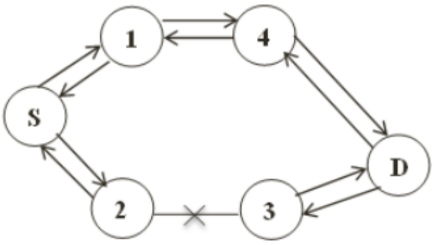

Figure 2. Architecture of Blackhole Attack

Figure 2 represents architecture of blackhole attack. In that, source node S wants to send packet to the destination node D. It first starts the route discovery process. Let us consider the node 3 is malicious node if it accepts request from S. It tells that it has shortest route to reach at destination node by replying to the source node S, if reply of node 3 reaches first than all other nodes to S. The node S assumes that route discovery is over and it rejects all the reply messages and starts sending packet to the node 3.As consequence of this all packets passing through node 3 is expended or vanishes.

Nital et. al. [16] proposed MOSAODV protocol. It uses heuristic approach to calculate total time source node waits for other reply packets after the first reply packets is received. There is one more table is inserted which adds the information of all replay packets. Source node discards those packets which have greater sequence number.

Limitation:-It assumes the key values of sequence number to spot malicious reply.

Grayhole Attack

Grayhole attack is enhancement of blackhole attack. In this type of attack the performance of malicious node is irregular. There are mainly three types of Grayhole attacks. In first type the malicious node may put packet at particular node and passes it to the other nodes. In second type the node may act as harmful node at any particular time but after some time it works as normal node. The third type of attack is fusion of above types of Grayhole attack that is, node may drop packet from any node for certain period of time only after that it behaves like other nodes. Because of these properties detection of Grayhole attack is very difficult task [12] [13].

Devu Manikantan Shila [17] proposed Channel aware detection algorithm that uses two methods for detecting malicious node. Hop-by-hop loss observation by next hop (downstream node) and traffic monitoring by previous hop (upstream node). There are several routes from a source to a destination. So the source may receive numerous route replies from a destination. The source node should able to cache these routes to moderate the overhead suffered during new route discovery process.

Limitation:- Problem of colliding multiple nodes with each other is not studied.

Sybil Attack

In this type of DOS attack, the attacker formulate multiple identities and behaves like different node instead of single these multiple identities referred to as Sybil identities or Sybil nodes [12] [13].

Tangpong A. and Kesidis G. [18] proposed a robust Sybil attack detection framework for MANET which is depends on cooperative monitoring of network activities. In this, each node in network observes a packet passing through it periodically exchanges its observation in order to determine the presence of an attack. Limitation:- The accuracy dropped when nodes moved faster because Sybil identifies were observed together less frequently.

Sinkhole Attack

In this type of DOS attack a negotiated node or malicious node announces incorrect route information to produce itself as a specific node and receives whole network traffic. It alters the private information, such as changes in data packet or put them to make network complex. A malicious node tries to attract a secure data from all neighboring nodes [12] [13].

Thanachai et.al. [19] proposed a trust weight scheme. This scheme assigns trust weights to all presented nodes. If a neighboring nodes fails to pass the massage the ad hoc node cuts its trust weight of any neighbor drops below a set threshold, the neighbor node is considered as doubtful node. The neighbor is referred to verify the suspicious node to be identified as a malicious node.

Limitation:- The schemes may not detect the malicious node in every situation.

Spoofing Attack

In spoofing attack attacker spoofs the identify of another node in network and thus it tries to receives the massages of the spoofed node. The attacker may even be attempting to reinstall the network and remove security events to allow subsequent attack [12] [13].

Masud et. al. [20] proposed location based detection approach that used signal direction in association with peer nodes to deliver the location of sender, which is used to determine spoofing attack. The solution does not rely on strength of the signal. Limitation:- It requires one trusted node and also increase the storage overhead.

Byzantine Attack

In this, a cooperated intermediates node or a set of cooperated intermediate nodes work in agreement and carries out attack such as creating routing loops, forwarding packets on non-optional path or selectively dropping packets. As consequence of these is interruption of routing services [12] [13].

Claude Crepeau [21] proposed a secure on-demand MANET routing protocol named Robust source routing(RSR) is capable of delivering packets to their corresponding destination though there is large extents of malicious agents are present which selectively drop packets they are required to forward. RSR also introduced concept of Forerunner (FR) which informs nodes along the path they should expect specified data flow within a given time frame. The path elements check the data flow and in that they do not receive traffic flow. They just send information to the source telling it that data flow they predicted did not arrived. By doing this the link having malicious agents can easily be identified that agent will be finally separated.

Limitation:-Increase in overhead as number of malicious node increases.

Modification Attack

This attack modifies packets and disrupts the overall communication network nodes. The attack also modifies the destination address in dynamic topology. Hence the packet unable to reach at the appropriate destination [12] [13].

Vaithiyanathan [22] proposed a scheme called key management. This scheme is implemented in Node Transaction Probability (NTP) protocol. This NTP algorithm affords bandwidth with higher utilization for the period of heavy traffic with less overhead. NTP fixes suitable routes using received power. The scheme detects the modification, impersonation attacks and TTL attacks and, prevents the effects of malicious node and decides correct methods to remove such malicious nodes in dynamic condition. Limitation: - NTP is not secure protocol therefore the packet delivery cannot be guaranteed.

Transport Layer Attack

Syn Flooding Attack

In this type of DOS attack a malicious node continuously send SYN packets to the target node. The target node sends SYN-ACK packets after receiving SYN packets. The packet which acknowledged these half-opened data structure rests in target node. The target node store these half-opened connection in fixed-size table but it expects the acknowledgement of three-way handshake all these pending could overflow the buffer and target node cannot receives any real users packets to open the connection [12] [13].

Ping et. al. [23] proposed a method of neighbor suppression that present request packet flooding. The node arranges the request according to priority rather than with FIFO (First In First Out). If the arriving packet crosses the frequency the node is assumed as attacker nodes and the target node stop the packets receiving from attacker node.

Limitation:- There increase in computing overhead to mobile node and when there heavy traffic such scheme is not effective.

Multiple Layer Attack

Jellyfish Attack

It is similar to blackhole attack. A Jellyfish attacker first interferes into forwarding group and postpones the data packets unreasonably for particular time before forwarding them. Though increase in end-to-end delay and lower the performance of the real application. It is targeted against closed loop flows such as TCP [12] [13].

Imad Aad [24] proposed a method to avoid Jellyfish attackby minimizing end-to-end delay.

Packet Drop Attack

The packet dropping attacks can interrupt the routing messages. In this attacks opponents collaborates as usual in the discovery process and introduces the constant packets dropping attacks if it contains as one of the intermediate nodes. In addition instead of constantly dropping the entire packet opponent may change their techniques using selective or periodic packets dropping packets to help their interrupting behavior remains canceled [12] [13].

Muhammad Zeshan [25] proposed two folded approach. The first approach will discover the misbehavior of nodes and also will classify the malicious happenings in the network and then after identification of nodes misbehavior in the network other approach will separate the malicious node from network.

Dos Attack

The basic aim of denial service of attack is to avoid genuine or real for using the network services. In DOS attack there is different scenario available the first scenario target to the memory, storage space or CPU of service provider. A node constantly sends flooding packets to its next node to jam the storage space the second scenario targets energy resources like battery power. A malicious node continuously sends the fake packets with aim of consuming battery. The third scenario targets the bandwidth. The attacker is located between multiple communicating nodes and wastes the network bandwidth [12] [13].

Soryal J. Used Markov [26] Chain is applicable using Bianchi's model to gain the possible number of maximum throughput when all users are authentic. This model has greater accuracy of theoretically computed throughput compared to simulated throughput under same condition.

Limitation:-We need to store MAC Address first into Table.

DDOS Attack

The DDOs attacks are both distributed and denial service attack. They are habitually large scale in the nature and can significantly weaken the performance of the victim network. In DDOS attack the attacker first constructs the network of harmful hosts which are usable for launching the attack. These harmful nodes are known as zombies are then mounted with attacking tools, which are able to carry out attack under the switch of the attacker [12] [13].

Prabha et.al. [27] proposed defense mechanism for DDOS attack is categorized into two main parts.

Limitation:- Analysis of proposed method has not been done.

2.5 CGA Related Work

The idea of using Cryptographically Generated Addresses first appeared in the Child-proof Authentication for MIPv6 (CAM) which was proposed by O'Shea and Roe [28]. In the CAM approach, the hash of the owner's public key is added to the interface ID portion of IPv6 address. However the drawback of this approach is, it is vulnerable to collision attack.

Montenegro and Castelluccia [29],worked on a similar proposal for Mobile IPv6, suggested an improvement and an extension to the CAM approach to make it more resistant to birthday collision by adding some "random" data to the hash input. But this method severely limits certain classes of denial of service attacks and hijacking attacks.

T. Aura [30], proposed the Hash Extension technique that increases the hash length beyond the 64-bit limit without actually increasing its length. The purpose of this method is to increase 64-bit value for protecting address for security point. This technique increases both the cost of generating a new CGA address and the cost of initiating a brute-force attack against the address.

C. Vogt, J. Arkko and W. Haddad [31],proposed a route optimization (RO) mechanism which is new and superior security based.It has given a home address ownership and a new care of address verification procedure via CGAs. Credit-Based Authorization (CBA) mechanism is used to guard against redirection-based flooding attack. The complete testing of care-of address is done before data packets are sent to that address to prevent flooding attacks. However, a "blocking" care-of-address test typically has detrimental impacts on handoff efficiency.

N. Hakiem [32], proposed a new scheme to manage IPV6 addresses in WLAN which may be implemented into DHCPv6 software each user will be assigned a group of IP addresses that are generated cryptographically using S-AES. Since S-AES is for academic purpose, it is an educational rather than a secure encryption algorithm also it is vulnerable with linear calculations therefore we should use AES which resistant against all known attacks instead of using S-AES.

Nashrul Hakiem [33], proposed the mechanism that uses checksum for validation of probability of coincidental match of randomly generated Interface Id or generated by some other mechanism. It is shown that collision probability of Interface Ids is definitely very small; even if we assume that maximum number of users within the enterprize connects to the same subnet ID.

Ahmad AlSa'deh, Hosnieh Raee [6], proposed the mechanism that used secure hash algorithm (SHA-I) has condition of 16*sec=0 to generate the CGA. The sec is nothing but security level which is 3-bit field that store 0 to 7 integer value. In that 0 means least secure and 7 means more secure. According to condition if value of sec=0 the algorithm succeed otherwise fails. By this accuracy is maintained but security is lost. Also it requires very large computational time to generate CGA.

2.6 Attacks on AES

AES is the best and strongest cryptology algorithm, because of three areas: security, cost, and implementation. AES is secure against many attacks like brute-force, differentialand linear attacks. But, there some attacks are still possible in AES.

In April 2005 D.J. Bernstein [34] proclaimed a cache timing attack that he used to break a custom server that used OpenSSL's AES encryption. The custom server was designed to give out as much timing information as possible, and the attack required over 200 million chosen plaintexts. However, limitation is same key is used to encrypt each block. Some researcher says the attack is not practical over the internet with a distance of one or more hops.

Warren D.Smith [35] describes a new powerful form of linear cryptanalysis. It appears to break AES. A small algorithm can quickly determining AES-256 keys from plaintextcipher text pairs exists. limitation is the attack's runtime is faster than exhaustive key search.

In 2011 A.Sekar, S.Radhika and K.Anand [36] propose a method to enhance the strength of the AES algorithm by increasing the key length to 512 bit and thereby the number of rounds is increased in order to provide a stronger encryption method for secure communication. Code optimization is done in order to improve the speed of encryption and decryption using the 512 bit AES. This method don't modify the structure of AES but only increase the number of rounds and so the attacks which need the same key are still serious to this algorithm at the same time this algorithm increase the processing time which will limit the use of AES in real application.

3. MODIFICATIONS

Based on related work, CGA is not complete security solution it still shows dimness's. It is vulnerable to different attack like collision attack, DOS attack, hijacking attack, and brute-force attack if, SHA-I algorithm is used. By these opinions, we are using the AES algorithm which is the best and strongest cryptology algorithm because of three areas: security,cost, and implementation. AES is secure against many attacks such that brute-force, differential and linear attacks. According to literature survey of Attacks on AES, we come to the point that, there are a lot of attacks on AES using different cryptanalysis techniques. So to resist these attacks we concerned on protection of AES structure against attacks and the most important attacks use the same cipher key for all encrypted blocks to complete the cryptanalysis steps, because it attacks the full round AES. For example, Daniel J. Bernstein needs 2×10^8 plaintext-ciphertext-time triples on the same key. This performs to attack failed if we changed the key with each block encryption. Depending on the idea we design our algorithm.

4. PROPOSED SYSTEM

As the MANETs are more susceptible to various security related attacks for communications. It brings down the overall performance of the network. Detecting attacks in a wireless ad hoc network requires attention. Many approaches employ security solution but that is in IPV4 technology while some other use encryption technology to prevent attacks. However, this hinder inherent the flexibility of wireless ad hoc network. Such a system requires large overhead and increases the complexity.

The IPV6 is prerequisite of upcoming because it is more secure than IPV4. To make IPV6 more powerful there is Cryptographically Generated Addresses (CGAs) method which was mainly intended to attest the address ownership and to advert stealing of existing IPV6 addresses by binding owner's public key to the generated addresses. Until now to generate CGA only SHA-I algorithm is used. According to Ahmad AlSa'deh, Hosnieh Raee [6] mechanism that used secure hash algorithm (SHA-I) has condition of 16*sec=0 to generate the CGA. The sec is nothing but security level which is 3-bit field that store 0 to 7 integer value. In that 0 means least secure and 7 means more secure. According to condition if value of sec=0 the algorithm succeed otherwise fails. By this accuracy is maintained but security is lost. Also it requires very large computational time to generate CGA. However, computing value of hash2 is pricey part of CGAs generation process. CGAs are not absolute security solution it still has paleness and susceptibilities to threats. CGAs are exposed to collision attacks. To make CGAs more privacy conscious use another techniques in CGAs that have excellent security, low resource consumption and can improve the efficiency by avoiding collision probability.

So that point of view, we are using the AES algorithm which is the best and strongest cryptology algorithm. By research AES is secure against many attacks such that brute force, differential and linear attacks. According to literature survey of Attacks on AES, we can conclude that, there are a lot of attacks on AES using different cryptanalysis techniques. So to resist these attacks we concerned on protection of AES structure against attacks and the most important attacks use the same cipher key for all encrypted blocks to complete the cryptanalysis steps, because it attacks the full round AES. For example, Daniel J. Bernstein need 2×10^8 plaintext-ciphertext-time triples on the same key. This performs to attack failed if we changed the key with each block encryption. Depending on the idea we use different sub keys from the symmetric real key and using each sub key to encrypt the one AES block and design our algorithm.

5. CONCLUSION

In this paper, the authors have studied various attacks in MANET, CGA related techniques, attacks on AES algorithm and concluded that, CGA is used to generate the private address in IPV6. CGA is vulnerable to collision attacks and is less secure if SHA-I algorithm is used to generate the same. AES algorithm can be used as an alternative to SHA-I algorithm. Because AES has excellent security, low resource consumption, high speed and ability to avoid collision attack. So, it will batter to use AES algorithm in CGA. As AES also suffers from some attacks, the modifications are required. The modification made in the AES algorithm may useful to generate different sub keys from the symmetric real key and using each sub key to encrypt the one AES block.

6. REFERENCES

[1] P. Goyal, V. Parmar, and R. Rishi, "Manet: Vulnerabilities, Challenges, Attacks, Application," IJCEM International Journal of Computational Engineering and Management, vol. 11. [Online]. Available: http://www.IJCEM.org

[2] M. Chinta, "Mobile ad hoc Networks (MANETs): Overview, Properties of a MANET, spectrum of MANET, applications, routing and various routing algorithms, security in MANET," Mobile Computing Unit-7 Mobile Ad Hoc Networks (MANETs), pp. 1–23. [Online]. Available: http://www.jntuworld.com

[3] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges." Ad Hoc Networks, vol. 1, no. 1, pp. 13–64, 2003. [Online]. Available:http://dblp.unitrier.de/db/journals/adhoc/adhoc1.html#ChlamtacCL03

[4] D. Durich and D. Montesinos, "AD-HOC NETWORKS," Telecommunication systems and networks.

[5] M. W. Murhammer and O. Atakan, “TCP/IP Tutorial and Technical Overview,” International Technical Support Organization. [Online]. Available: http://www.redbooks.ibm.com.

[6] A. Alsadeh, H. Rafiee, and C. Meinel, “Cryptographically Generated Addresses (CGAs): Possible Attacks and Proposed Mitigation Approaches,” Computer and Information Technology, International Conference on, vol. 0, pp. 332–339, 2012.

[7] F. J. Galera, P. M. Ruiz, A. F. Gomez-skarmeta, and A. Kassler, “Security Extensions to MMARP Through Cryptographically Generated Addresses.” in Lecture Notes on Informatics, 2005, pp. 339–342.

[8] N. Hakiem, M. U. Siddiqi, and H. M. Rafiq, “Simulation Study of a Many-to-One Mapping for IPv6 Address Owner Identification in an Enterprise Local Area Network,” International Journal of Network Security, vol. 0, pp. 1–8, Nov 2013.

[9] A. Jagadev and V. Senapati, “Advanced Encryption Standard (AES) Implementation,” Department of Electronics and Communication Engineering National Institute of Technology, Rourkela, May 2009.

[10] M. D. Saravanan and M. I. Anbumuthu, “A Novel Node Security Mechanism For Mobile Ad-Hoc Network,” International Conference on Engineering Technology and Science (ICETS’14), vol. 3, pp. 463–467, Feb 2014.

[11] S. Sahmoud, W. Elmasry, and S. Abudalfa, “Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher.” International Arab Journal of e-Technology, vol. 3, no. 1, pp. 17–26, 2013. [Online]. Available: http://dblp.unitrier.de/db/journals/iajet/iajet3.html#SahmoudEA13

[12] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication,” pp. 265–274, 2009.

[13] K. Sahadevaiah and P. R. P.V.G.D, “Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks,” Network Protocols and Algorithms, vol. 03,no. 4, pp. 265–274, 2011. [Online]. Available: http://www.macrothink.org/npa

[14] A. Hamieh and J. Ben-Othman, “Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution,” in IEEE International Conference on Communications (ICC), 2009. [Online].Available:http://ieeexplore.ieee.org/xpls/absall.jsp?arnumber=5198912

[15] Y. chun Hu, A. Perrig, and D. B. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE Journal on Selected Areas in Communications, vol. 24, pp. 370–380, 2006.

[16] N. Mistry, D. C. Jinwala, and M. Zaveri, “Improving AODV Protocol Against Blackhole Attacks,” in Proceedings of the International Multi Conference of Engineers and Scientists.

[17] D. M. Shila, Y. Cheng, and T. Anjali, “Channel Aware Detection of Gray Hole Attacks in Wireless Mesh Networks.” in GLOBECOM. IEEE, 2009, pp.1–6.[Online].Available:http://dblp.unitrier.de/db/conf/globecom/globecom2009.html#ShilaCA09

[18] A. Tangpong, G. Kesidis, H.-Y. Hsu, and A. R. Hurson,“Robust Sybil Detection for MANETs.” in ICCCN. IEEE,2009, pp. 1–6. [Online]. Available: http://dblp.unitrier.de/db/conf/icccn/icccn2009.html#TangpongKHH09.

[19] T. Thumthawatworn, T. Yeophantong, and P. Sirikriengkrai,“Adaptive sinkhole detection on wireless ad hoc networks,” in Aerospace Conference, 2006 IEEE. IEEE, 2006, pp. 10–pp.

[20] M. M. Rana, K. E. U. Ahmed, N. R. Sumel, M. S. Alam, and L. Sarkar, “Security in Ad Hoc Networks: A Location Based Impersonation Detection Method,” Computer Engineering and Technology, International Conference on, vol. 2, pp. 380–384, 2009.

[21] C. Crepeau, C. R. Davis, and M. Maheswaran, “A Secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes,” in Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops - Volume 02, ser. AINAW ’07. Washington, DC,USA: IEEE Computer Society, 2007, pp. 19–26. [Online].Available:http://dx.doi.org/10.1109/AINAW.2007.54

[22] Vaithiyanathan, R. G. Sheeba, E. E. N., and S. Radha, “A Novel Method for Detection and Elimination of Modification Attack and TTL Attack in NTP Based Routing Algorithm,” in Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, ser. ITC ’10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 60–64. [Online]. Available:http://dx.doi.org/10.1109/ITC.2010.23

[23] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, “Resisting Flooding Attacks in Ad Hoc Networks.” in ITCC (5). IEEE Computer Society, 2005, pp. 657–662. [Online].Available:http://dblp.unitrier.de/db/conf/itcc/itcc2005-2.html#YiDZZ05

[24] I. Aad, J.-P. Hubaux, and E. W. Knightly, “Denial of Service Resilience in Ad hoc Networks,” in Proceedings of the 10th annual international conference on Mobile computing and networking, ser. MobiCom ’04. New York, NY, USA: ACM, 2004,pp.202–215.[Online].Available: http://doi. acm.org/10.1145/1023720.1023741

[25] M. Zeshan, S. A. Khan, A. R. Cheema, and A. Ahmed, “Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks,” in Future Information Technology and Management Engineering, 2008. FITME’08. International Seminar on. IEEE, 2008, pp. 568–572.

[26] J. Soryal and T. Saadawi, “IEEE 802.11 Denial of Service Attack Detection in MANET,” in Wireless Telecommunications Symposium (WTS), 2012. IEEE, 2012, pp. 1–8.

[27] N. Sharma, B. Raina, P. Rani, Y. Chaba, and Y. Singh, “Attack Prevention Methods For DDOS Attacks In MANETS,” ASIAN JOURNAL OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY, vol. 1, no. 1, 2013.

[28] G. O’Shea and M. Roe, “Child-Proof Authentication for MIPv6 (CAM),” Computer Communication Review,vol.

31, no. 2, pp. 4–8, 2001. [Online]. Available:http://dblp.uni-trier.de/db/journals/ccr/ccr31.html#OSheaR01

[29] G. Montenegro and C. Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses," 2002.

[30] T. Aura, "Cryptographically Generated Addresses (CGA),"RFC 3972 (Proposed Standard), Internet Engineering Task Force, March 2005, updated by RFCs 4581, 4982. [Online].Available: http://www.ietf.org/rfc/rfc3972.txt

[31] C. Vogt, W. Haddad, and J. Arkko, "Aplying Cryptographically Generated Addresses and Credit-Based Authorization to Mobile IPv6," Internet Draft, IETF, 2006.

[32] N. Hakiem, A. Priantoro, M. Siddiqi, and T. Hasan, "Generation of Cryptographic One-to-Many Mapping IPv6 Address using S-AES," in Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on. IEEE, 2010, pp. E13–E18.

[33] N. Hakiem, M. U. Siddiqi, and S. P. W. Jarot, "Collision Probability of One-to-Many Reversible Mapping for IPv6 Address Generation," in Computer and Communication Engineering (ICCCE), 2012 International Conference on. IEEE, 2012,pp. 599–602.

[34] D. J. Bernstein, "Cache-Timing Attacks on AES," April 2005.

[35] W. D. Smith, "1. AES seems weak. 2. Linear time secure cryptography." IACR Cryptology ePrint Archive, vol. 2007,p. 248, 2007. [Online]. Available:http://dblp.unitrier.de/db/journals/iacr/iacr2007.html#Smith07

[36] Sekar.A, Radhika.S, and Anand.K, "Secure Communication using 512 Bit Key," European journal of Scientific Research, vol. 52, no. 1, pp. 61–65, 2011.